PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 18-4673

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

v.

ROBERT MICHAEL FALL,

Defendant - Appellant.

Appeal from the United States District Court for the Eastern District of Virginia, at Norfolk. Henry Coke Morgan, Jr., Senior District Judge. (2:17-cr-00012-HCM-DEM-1)

Argued: December 10, 2019 Decided: April 3, 2020

Before DIAZ and QUATTLEBAUM, Circuit Judges, and Max O. COGBURN, United States District Judge for the Western District of North Carolina, sitting by designation.

Affirmed by published opinion. Judge Quattlebaum wrote the opinion in which Judge Diaz and Judge Cogburn joined.

ARGUED: Mark Diamond, Richmond, Virginia, for Appellant. Elizabeth Marie Yusi, OFFICE OF THE UNITED STATES ATTORNEY, Norfolk, Virginia, for Appellee. **ON BRIEF:** G. Zachary Terwilliger, United States Attorney, Daniel T. Young, Assistant United States Attorney, OFFICE OF THE UNITED STATES ATTORNEY, Alexandria, Virginia, for Appellee.

QUATTLEBAUM, Circuit Judge:

Robert Michael Fall asks us to reverse his conviction of receipt, possession and transportation of child pornography for four reasons. First, he claims that the Virginia Beach Police Department (the "VBPD") violated his Fourth Amendment rights in the way it searched his laptop computer. Second, he asserts the counts against him for receipt and possession of child pornography produced improper multiplicity. Third, he argues that moving images from one's laptop to one's Dropbox account does not amount to transportation of child pornography. And fourth, he contends that the presence of child pornography images in temporary storage files on a laptop computer does not sufficiently prove knowing receipt of child pornography because such images can be saved through inadvertent internet use. These arguments require us to apply well-settled principles of criminal law to the realities of modern technological advancements in computers and the internet. While we agree with Fall that personal computing devices like laptops and cell phones implicate privacy interests about which we must exercise care, upon considering this record, we find no reversable error by the district court. Accordingly, we affirm.

I.

Fall was living with his parents in Virginia Beach, Virginia when he invited his niece, S.D., to stay with them. While S.D. and her boyfriend were watching television in the guest bedroom, they noticed a laptop computer partially visible under the guest bed. S.D.'s boyfriend opened the laptop and discovered at least one image of child pornography. S.D. then observed several pictures of children visible on the laptop's home screen, as well

as a "sexually explicit" video of a child. J.A. 77. Continuing to examine the contents of the computer, S.D. also discovered "mechanic stuff," leading her to believe that the laptop belonged to Fall—who owned an auto repair shop. J.A. 77.

S.D. then went into Fall's bedroom, where she saw another laptop. After opening it, she discovered additional child pornography images. She left that laptop in her uncle's bedroom and drove the laptop from the guest bedroom to the local VBPD station.

While meeting with Officer James Mockenhaupt at the police station, S.D. showed him some of the images of child pornography on the laptop. Officer Mockenhaupt then contacted a VBPD Special Victims Unit detective, who instructed him to send S.D. to the VBPD headquarters.

There, S.D. met with Detectives Patrick Henderson and Ryan Sweeney. After S.D. explained what she had seen on the laptop, Detective Henderson opened it and observed thumbnail "icons on the desktop that appeared to be nude individuals." J.A. 95. He thought the images could have depicted children. Detective Henderson then clicked on two video thumbnails on the laptop's home screen, both of which depicted child pornography.[1]

Detectives Henderson and Sweeney drove to Fall's auto repair shop to interview him. After receiving *Miranda* warnings, Fall invoked his right to counsel and refused consent for a search of his residence. The detectives then began drafting an affidavit for a

[1] At trial, the parties stipulated that the laptop "contain[ed] images and at least two videos of child pornography. . . ." J.A. 645.

search warrant. Officer Mockenhaupt traveled to Fall's residence to secure the scene. While Mockenhaupt was there, Fall arrived at the house, picked up his mother and left.

Subsequently, neighbors told Officer Mockenhaupt that they saw a man crawl out of Fall's second-story window behind the house, throw something on top of the lower-level roof and then jump off the roof and flee. They did not recognize the man.

When Officer Mockenhaupt investigated, he discovered a laptop on the lower-level roof. Fearing rain, he and another officer secured the laptop in the second-floor bathroom until police could execute a search warrant.

The completed affidavit submitted with the warrant application stated,

> On August 4th, 2016, this affiant met with [S.D.] at Police HQ. [S.D.] is temporarily living at [redacted] in the city of Virginia Beach with her uncle, Robert Fall. . . . Under the bed in the room she is staying in, she discovered a laptop. She opened the laptop to see if it was operable and immediately noticed on the desktop several icons which appeared to be of pornography. She opened at least one file and saw that it was child pornography. She brought the laptop to this affiant at police headquarters. Detective Henderson and this affiant spoke with [S.D.] and Detective Henderson viewed two files on the desktop computer. One file depicted a female approximately 10-12 years old kneeling next to a man masturbating. The other video was of a 10-12 year old girl masturbating completely naked while lying on the floor. [S.D.] mentioned she believes the computer belongs to her uncle because there were programs on the computer indicative of mechanical knowledge and her uncle owns a mechanic shop. She then went into her uncle's bedroom and found a laptop. When looking at that laptop, she described that on the desktop of the computer she saw a thumbnail with a naked girl on it. . . . Prior to this occasion an individual matching Mr. Fall's clothing description and identified by a neighbor as Mr. Fall was seen exiting the residence at [redacted] and throwing a laptop computer on the roof of the residence before exiting the yard.

J.A. 65.

After obtaining a warrant later that evening, the VBPD searched Fall's residence. The VBPD seized various pieces of electronic evidence during the search, including the laptop recovered from the roof, another laptop from the defendant's closet and numerous compact discs from Fall's bedside table. All these items contained videos and images of child pornography.

A federal grand jury in Norfolk, Virginia indicted Fall on five counts of receipt and attempted receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2); one count of transportation of child pornography, in violation of 18 U.S.C. § 2252(a)(1); and three counts of possession of a matter containing child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B). Upon the government's motion, the district court dismissed two of the receipt counts and one of the possession counts.

Fall moved to suppress the physical evidence seized during the search of his residence, arguing that it was the product of an improper search of the laptop that S.D. found in the guest bedroom. He argued that the third-party consent doctrine did not apply to the search of his computer or his residence, and that the VBPD's search of the laptop extended beyond the private search of S.D. and her boyfriend. According to Fall, the information gained from this illegal search tainted the search warrant and, thus, the physical evidence obtained from his residence under that warrant. He also claimed that the warrant application improperly represented that Fall's neighbor reported seeing Fall on the roof of his residence when she merely said she saw a person on the roof.

The district court denied the motion, concluding "there is no evidence to suggest that Detective Henderson expanded the search beyond that which was needed to verify the

report by the private citizen S.D. Instead, it appears from the evidence that Detective Henderson was merely verifying that what S.D. found was actually child pornography." J.A. 642. The district court also found that the alleged misrepresentation about Fall being seen on the roof was merely an error resulting from a miscommunication from one law enforcement officer to another, the reliance on which did not "constitute 'reckless disregard for the truth.'" J.A. 643. The court further found that the statement was not necessary to obtain the search warrant.

Fall was tried on six counts from the indictment: Counts 3, 4 and 5, which each charged him with receipt and attempted receipt of a single image of child pornography; Count 6, which charged him with transportation of child pornography by uploading a video of child pornography from his laptop to an online file-storage account; and Counts 7 and 8, which charged him with possession of child pornography on the roof laptop and the compact discs. The jury found Fall guilty on all counts.

Prior to sentencing, the government moved to dismiss Counts 7 and 8 to minimize any potential double jeopardy issues on appeal. The district court granted the government's motion to dismiss Count 8, but denied it as to Count 7. It reasoned that the high degree of factual overlap between the images on the discs in Count 7 and the roof laptop in Count 7 was significant enough to merit the dismissal of Count 8. It then compared the images in Count 7 with those identified in Counts 3, 4 and 5. It found that the degree of overlap was so small that the dismissal of Count 7 would be inappropriate.

Fall was sentenced to 96 months of imprisonment on Counts 3, 4, 5, 6 and 7—to run concurrently—and 20 years of supervised release. Fall filed a timely notice of appeal. We have jurisdiction over the appeal pursuant to 28 U.S.C. § 1331.

II.

Fall first argues that the physical evidence should have been suppressed as fruit of the poisonous tree—the improper warrantless search of his computer that S.D. and her boyfriend found in the guest bedroom and took to the VBPD. According to Fall, without that search, the VBPD could not have obtained the warrant to search his home, and the physical evidence would not have been discovered.

When "reviewing a district court's ruling on a motion to suppress, this Court 'review[s] conclusions of law de novo and underlying factual findings for clear error.'" *United States v. Clarke*, 842 F.3d 288, 293 (4th Cir. 2016) (quoting *United States v. Banks*, 482 F.3d 733, 738 (4th Cir. 2007)). If, as here, the district court denied the motion to suppress, this Court "construe[s] the evidence in the light most favorable to the government." *Id*. (quoting *United States v. Kelly*, 592 F.3d 586, 589 (4th Cir. 2010)).

Fall argues the district court erred in concluding that the officers did not expand S.D.'s private search of the laptop. Thus, according to Fall, the private search exception to the Fourth Amendment does not apply here. The private search doctrine is based on the principle that the Fourth Amendment does not protect against searches conducted by private individuals acting in a private capacity. *United States v. Richardson*, 607 F.3d 357, 364 (4th Cir. 2010). And since the Fourth Amendment is not implicated by a private search,

it is not violated when the police merely review the same information that was discovered during the private search. *See id*. Thus, when a third party provides the police with evidence that she obtained in the course of her own search, the police need not "stop her or avert their eyes." *Coolidge v. New Hampshire*, 403 U.S. 443, 489 (1971).

The seminal private search doctrine case is *United States v. Jacobsen*, 466 U.S. 109 (1984). There, Federal Express employees saw a damaged box, opened it and found suspicious bags of white powder packaged inside a tube. *Id*. at 111. The employees notified the United States Drug Enforcement Agency ("DEA") and placed the bags and tube back inside the box. *Id*. Upon the DEA agent's arrival, he removed the bags from the box and then tested the powder to confirm it was cocaine. *Id*. at 111–12. The Supreme Court held, in part, that no Fourth Amendment search occurred when the DEA agent removed the bags from the box, because "the removal of the plastic bags from the tube and the agent's visual inspection of their contents enabled the agent to learn nothing that had not previously been learned during the private search." *Id*. at 120.

Although the testing of the powder went beyond the private search, the Court established that "additional invasions of respondents' privacy by the government agent must be tested by the degree to which they exceeded the scope of the private search." *Id*. at 115. There, the Court held that the DEA agent's field test of the narcotics was permissible because a "chemical test that merely discloses whether or not a particular substance is cocaine does not compromise any legitimate interest in privacy." *Id*. at 123 (reasoning that "governmental conduct that can reveal whether a substance is cocaine, and no other arguably 'private' fact, compromises no legitimate privacy interest" because "Congress

has decided . . . to treat the interest in 'privately' possessing cocaine as illegitimate"). *See also United States v. Kinney*, 953 F.2d 863 (4th Cir. 1992) (holding that the manipulation by the police of guns discovered by a private citizen to the extent necessary for the police to obtain the serial numbers was a permissible private search because "[t]here [was] no analytically significant reason to view the recording of gun serial numbers in the present case any differently from the drug field test in *Jacobsen*").

While we have not addressed the private search doctrine in the context of electronic devices, our sister circuits have utilized varying approaches when confronted with this issue. The Eleventh and Sixth Circuits have held that there must be an exact one-to-one match between electronic files viewed by a private party and files later examined by police. Even if the police's extension of the search is de minimis, it loses the protection of the private search exception. *See United States v. Sparks*, 806 F.3d 1323 (11th Cir. 2015); *United States v. Lichtenberger*, 786 F.3d 478 (6th Cir. 2015).

But, as the government points out, other circuits have allowed a more permissive application of the private search doctrine to electronic searches. The Seventh and Fifth Circuits have held that with respect to officers searching containers that were not examined by the private party, a more expansive officer search "would not necessarily be problematic if the police knew with substantial certainty, based on the statements of the private searches, their replication of the private search, and their expertise, what they would find inside." *United States v. Runyan*, 275 F.3d 449, 464 (5th Cir. 2001); *see Rann v. Atchison*, 689 F.3d 832, 838 (7th Cir. 2012). *Runyan* also held that the police do not exceed the private search when they examine more items within a closed container than did the private

searchers. *Runyan*, 275 F.3d at 464. The reasoning behind this view relates more to access to the device in general than the specific information reviewed. Since the private party accessed the device, these courts reason that so too can the police. *Id*.

We need not determine today the outer boundaries of the private search doctrine in the context of electronic searches for this Circuit because even if the search was not proper under the private search exception, the denial of the motion to dismiss should be affirmed under the good faith exception to the exclusionary rule. Under that exception, "evidence obtained by an officer who acts in objectively reasonable reliance on a search warrant will not be suppressed, even if the warrant is later deemed invalid." *United States v. Thomas*, 908 F.3d 68, 72 (4th Cir. 2018) (citing *United States v. Leon*, 468 U.S. 897, 922 (1984)). "[E]vidence obtained from an invalidated search warrant will be suppressed only if 'the officers were dishonest or reckless in preparing their affidavit or could not have harbored an objectively reasonable belief in the existence of probable cause.'" *United States v. Lalor*, 996 F.2d 1578, 1583 (4th Cir. 1993) (quoting *Leon*, 468 U.S. at 926). Further, the exception may apply even where a search warrant is "facially deficient" as long as "the warrant . . . was not so facially deficient as to preclude reasonable reliance upon it . . . ." *United States v. Dickerson*, 166 F.3d 667, 694–95 (4th Cir. 1999), *reversed on other grounds by Dickerson v. United States*, 530 U.S. 428 (2000). "[U]ncontroverted facts known to [the officer] but inadvertently not presented to the magistrate" are an important part of this inquiry. *United States v. Lyles*, 910 F.3d 787, 797 (4th Cir. 2018) (internal quotation marks omitted).

The warrant here is not facially deficient, much less to the extent required to preclude reasonable reliance on it. The affidavit submitted to obtain the warrant contained much more information than Detective Henderson's description of what he saw on the laptop. Specifically, the affidavit contained S.D.'s statements about personally observing child pornography on the defendant's laptop and the neighbor's statement about a man throwing a laptop on the roof of Fall's residence. Removing Detective Henderson's potentially problematic observations, the affidavit would have contained the following information:

> On August 4th, 2016, this affiant met with [S.D.] at Police HQ. [S.D.] is temporarily living at [redacted] in the city of Virginia Beach with her uncle, Robert Fall. . . . Under the bed in the room she is staying in, she discovered a laptop. She opened the laptop to see if it was operable and immediately noticed on the desktop several icons which appeared to be of pornography. She opened at least one file and saw that it was child pornography. She brought the laptop to this affiant at police headquarters. . . . [S.D.] mentioned she believes the computer belongs to her uncle because there were programs on the computer indicative of mechanical knowledge and her uncle owns a mechanic shop. She then went into her uncle's bedroom and found a laptop. When looking at that laptop, she described that on the desktop of the computer she saw a thumbnail with a naked girl on it. . . . Prior to this occasion an individual matching Mr. Fall's clothing description and identified by a neighbor as Mr. Fall was seen exiting the residence at [redacted] and throwing a laptop computer on the roof of the residence before exiting the yard.

J.A. 65. This information provides an objectively reasonable basis for the officers to objectively believe that probable cause existed. *See Simmons v. Poe*, 47 F.3d 1370, 1378 (4th Cir. 1995) ("[T]he case law establishes that, even if an affidavit supporting a search warrant is based in part on some illegal evidence, such inclusion of illegal evidence does not taint the entire warrant if it is otherwise properly supported by probable cause.").

Aside from the information reflecting Detective Henderson's search of the laptop, the only other criticism lodged by Fall to the affidavit requesting the warrant relates to the erroneous statement that the neighbors observed Fall throw the laptop on the roof.[2] We agree the record indicates the neighbors did not identify Fall. They instead said a man on the roof of Fall's residence threw a laptop on the roof. But we also agree with the district court that the error does not constitute evidence of dishonesty or recklessness in preparing the affidavit. Accordingly, we agree with the district court that the record supports the application of the good faith exception.[3]

III.

Fall next claims that Count 7, which charged him with possession of child pornography, was multiplicitous of Counts 3, 4 and 5 charging him with receiving child pornography. Count 7 alleged that Fall "did knowingly possess one or more matters, that is, [the roof] laptop computer and the hard drive contained therein, . . . which contained visual depictions . . . . [that] involved the use of minors . . . engaging in sexually explicit

[2] While Fall pressed this issue below, he gives it scant attention on appeal. In fact, he may have abandoned the issue. *See Brown v. Nucor Corp.*, 785 F.3d 895, 923 (4th Cir. 2015). But even considering this error, we have no difficulty determining the good faith exception applies.

[3] The government argues that the independent source doctrine provides an alternative basis for affirming the district court's denial of Fall's motion to dismiss. Since we affirm the district court based on the good faith exception to the exclusionary rule, we decline to address that alternative argument or the perhaps more applicable inevitable discovery doctrine.

conduct," in violation of 18 U.S.C. § 2252(a)(4)(B). J.A. 24. Counts 3 through 5, meanwhile, alleged that Fall "knowingly receive[d] and attempted to receive" three images containing child pornography, in violation of 18 U.S.C. § 2252(a)(2). J.A. 20–22. The images charged in Counts 3 through 5 were present in space allocated to temporary internet files[4] on the roof laptop. Thus, Fall contends that the three images identified in Counts 3 through 5 could have also been stored on the roof laptop and hard drive mentioned in Count 7. As a result, according to Fall, the charges are multiplicitous.

"Multiplicity is 'the charging of a single offense in several counts.'" *United States v. Lawing*, 703 F.3d 229, 236 n.7 (4th Cir. 2012) (quoting *United States v. Burns*, 990 F.2d 1426, 1438 (4th Cir. 1993)). The Fifth Amendment's Double Jeopardy Clause prohibits multiplicitous indictments for crimes that "are in law and in fact the same offense." *United States v. Schnittker*, 807 F.3d 77, 81 (4th Cir. 2015) (quoting *United States v. Crew*, 538 F.2d 575, 577 (4th Cir. 1976)).

[4] At trial, Special Agent Joseph explained the concept of temporary internet files to the jury:

> Temporary internet files are maintained in the registry in multiple locations. They're going to cache when the user goes out into the internet. The data from a website is going to be stored in the computer's temporary internet files, and the reason for this is so that, when you go to that website again, it will load quicker because the operating system knows to just pull some of the data from the temporary internet files versus loading it all over again.

J.A. 410.

Importantly, however, Fall did not raise this argument by pretrial motion, as required by Federal Rule of Criminal Procedure 12(b)(3)(B)(ii). Thus, his argument is untimely.

The circuits that have addressed the question are split as to whether to review an unpreserved challenge to a multiplicitous indictment for plain error or whether the claim is altogether waived. While we have not previously addressed this issue, we need not weigh in on this split today because Fall's argument fails even under plain error review.

There is plain error only when "(1) an error was made; (2) the error is plain; (3) the error affects substantial rights; and (4) the error seriously affects the fairness, integrity, or public reputation of judicial proceedings." *United States v. Harris*, 890 F.3d 480, 491 (4th Cir. 2018). The first part of this test—the requirement that an error be made—is fatal to Fall's argument.

Charges cannot be multiplicitous where they are "based on two distinct offenses, occurring on two different dates, and proscribed by two different statutes." *United States v. Bobb*, 577 F.3d 1366, 1375 (11th Cir. 2009), *cited favorably in United States v. Schnittker*, 807 F.3d 77, 81 (4th Cir. 2015). Applied here, Fall was convicted under two separate statutes for distinct conduct. Under Count 7, he was convicted of possessing child pornography on August 4, 2016, the date of the warrant execution. And under Counts 3 through 5, he was convicted of knowingly receiving child pornography in January 2016—the date he received those images. Because these convictions involve different conduct on different dates, they are not multiplicitous.

While Fall claims *United States v. Schnittker*, 807 F.3d 77 (4th Cir. 2015) supports his multiplicity argument, it actually cuts against him. In explaining the general multiplicity rule, *Schnittker* explained that the Double Jeopardy Clause only prohibits convicting a defendant for two crimes that "are in law and in fact the same offense." *Schnittker*, 807 F.3d at 81 (quoting *United States v. Crew*, 538 F.2d 575, 577 (4th Cir. 1976)). Thus, *Schnittker* reasoned, two propositions can be true at the same time. First, it may be the case "that possession of child pornography is a lesser-included offense of receipt of child pornography." *Id*. Second, two charges for possessing and receiving images of child pornography might not actually be "the same in fact." *Id*. at 82. To determine the degree of factual overlap between two related counts, courts review "'the entire record' of the proceedings." *Id*. (quoting *United States v. Benoit*, 713 F.3d 1, 17 (10th Cir. 2013)).

Schnittker went on to conclude that no multiplicity problem arose from convicting a defendant of possessing images found on one hard drive and receiving videos found on a second hard drive, even when those same videos appeared on both drives. This was because "the defendant admitted to possessing over one thousand images or videos of child pornography, at least some of which did not ground the receipt conviction." *Id*. at 83. This supported the inference "that 'the possession conviction was based on an image the receipt of which did not form the basis of the receipt conviction.'" *Id*. (quoting *United States v. Polouizzi*, 564 F.3d 142, 159 (2d Cir. 2009)).

The same inference applies here. The evidence below established that the roof laptop contained four videos and 726 images of child pornography. The district court properly noted that "any overlap between [Counts 3, 4 and 5] and Count 7 is much too

small to warrant a finding that the offense conduct charged in Count 7 was in fact the same as that charged in the receipt counts." J.A. 707. And because the district court did not err, Fall cannot satisfy the first requirement of the plain error test. Thus, Fall's multiplicity argument fails.

IV.

Fall next argues that there was insufficient evidence for a reasonable jury to find that he transported a pornographic video under Count 6. While acknowledging that he moved a video containing child pornography from his laptop to a Dropbox account, Fall contends that the district court improperly denied his motion for acquittal because there was no evidence that he shared, attempted to share or even intended to share the video.

But as with his multiplicity argument, Fall failed to properly preserve this issue. Although he moved for acquittal on Count 6 after the close of the government's case, Fall failed to renew the motion after trial. Thus, this argument, which we would normally review de novo, is waived. *See United States v. Chong Lam*, 677 F.3d 190, 200 & n.10 (4th Cir. 2012) (holding that "[w]hen a defendant raises specific grounds in a Rule 29 motion, grounds that are not specifically raised are waived on appeal," unless a "manifest miscarriage of justice" has occurred).

But even if this claim was not waived, Fall's argument is without merit. Fall improperly conflates the offense of transportation with the offense of distribution. Transportation, which is the basis of Count 6, does not require conveyance to another person. For example, in *United States v. Ickes*, 393 F.3d 501, 504 (4th Cir. 2005), we

affirmed a transportation conviction based on the transportation of child pornography by automobile from Canada to Virginia without evidence of distribution to a third party. Moreover, other circuits have held that simply uploading child pornography to a website constitutes transportation. *See United States v. Davis*, 859 F.3d 429, 432, 434 (7th Cir. 2017) (affirming that a defendant transported child pornography when he "knowingly uploaded the pornographic images to Shutterfly," an "online photo-sharing website"); *United States v. Clingman*, 521 F. App'x 386, 393, 396 (6th Cir. 2013) (affirming transportation conviction where the government established that defendant uploaded child pornography to a website). Because the government established Fall transported child pornography from his laptop's hard drive to an online file-sharing website, his transportation charge was based on sufficient evidence. This remains true even if the government presented no evidence that anyone other than Fall accessed the file-sharing account.

Last, Fall's use of the internet in the transmission of child pornography satisfies the interstate commerce element of 18 U.S.C. § 2252 A(a)(1). *United States v. Miltier*, 882 F.3d 81, 87 (4th Cir.), *cert. denied*, 139 S. Ct. 130 (2018). Thus, we believe the record supports Fall's conviction on Count 6.

V.

Finally, Fall argues that there was insufficient evidence to convict him for receipt of child pornography in Counts 3, 4 and 5. He claims that because the images charged in these Counts were stored in the roof laptop's temporary internet files, it is possible they

appeared at the bottom of a webpage and downloaded onto his computer without his knowledge.

When reviewing the sufficiency of the evidence supporting a count of conviction, this Court considers whether "there is substantial evidence, taking the view most favorable to the Government, to support it." *Glasser v. United States*, 315 U.S. 60, 80 (1942), *abrogated on other grounds by Bourjaily v. United States*, 483 U.S. 171 (1987). "[T]he relevant question is whether, after viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *Jackson v. Virginia*, 443 U.S. 307, 319 (1979). We "consider circumstantial as well as direct evidence, and allow the government the benefit of all reasonable inferences from the facts proven to those sought to be established." *United States v. Savage*, 885 F.3d 212, 219–20 (4th Cir. 2018) (internal quotation marks omitted).

At trial, Fall pressed the same argument that he advances here extensively before the jury. He cross-examined the government's forensic examiner on this topic. During cross-examination and in his closing, Fall argued that the images charged in Counts 3 through 5 might have appeared at the bottom of a webpage, and if he failed to scroll down to view the entire website, his laptop may have cached these images without him realizing they were there. Fall's assertions depended heavily on the assumption that he was a technological novice so lacking in sophistication that his receipt of child pornography via the internet might have been accidental.

The government's evidence offered a different explanation—that Fall was a savvy collector of child pornography who had been seeking it out on the internet for well over a

decade. The government presented evidence establishing that Fall amassed child pornography across multiple laptops and storage devices. The roof laptop contained 726 images and four videos of child pornography. Another laptop recovered from his house contained 134 images of child pornography. Fall possessed 1,967 images and 21 videos of child pornography on eight CDs and DVDs. Finally, Fall's Dropbox contained 323 images and 2,992 videos. After being presented with all the evidence and hearing arguments from both parties, the jury adopted the position advocated by the government. While the jury was entitled to believe Fall's version, it was also entitled—after being charged that it must find that Fall knowingly received the images in order to convict him on these Counts— to believe that Fall's receipt was knowing based on the circumstantial evidence presented about his long-standing and extensive collection of child pornography on multiple devices. *See United States v. Pruitt*, 638 F.3d 763, 767 (11th Cir. 2011) ("Sufficient evidence supported the conviction on Count Two given the totality of other evidence in this case, including the evidence that Defendant had admittedly sought out and viewed child pornography on an entirely different computer around the same time.").

In considering whether there is sufficient evidence to support the jury's finding, we agree with Fall that the government offered no specific evidence tying contraband images located in the computer's temporary internet files to specific browsing activity or particular web searches. But we do not require direct evidence that Fall sought out and acquired these specific images. In criminal trials, a defendant's knowledge "will be provable (as knowledge must almost always be proved) by circumstantial evidence." *United States v. Santos*, 553 U.S. 507, 521 (2008). We see no reason that general principle would not apply

in child pornography cases. Indeed, many of our sister circuits have affirmed child pornography convictions based on circumstantial evidence of the defendant's history and involvement with child pornography. *See, e.g.*, *United States v. Manning*, 738 F.3d 937, 946 (8th Cir. 2014) (finding that defendant's "extensive knowledge of, and interest in, child pornography, were probative as circumstantial evidence regarding [his] knowing possession" of child pornography); *United States v. Hardrick*, 766 F.3d 1051, 1057 (9th Cir. 2014) (finding that "circumstantial evidence of [defendant's] knowledge was sufficient" to prove that he received child pornography); *United States v. Breton*, 740 F.3d 1, 17 (1st Cir. 2014) ("[A] defendant's history of visits to websites with a child pornography connection or use of search terms associated with child pornography can support a finding that the defendant knew the images he retrieved contained child pornography.").

In response, Fall relies primarily on the Tenth Circuit's decision in *United States v. Dobbs*, 629 F.3d 1199 (10th Cir. 2011). There, the government charged the defendant with receipt of child pornography images found in his temporary internet files. *Id*. at 1201. At trial, "the forensic specialist testified that a pattern existed wherein the arrival of suspect images on [the defendant's] computer was immediately preceded by searches using terms typically affiliated with child pornography." *Id*. at 1202. Relying on this evidence, the government argued that the defendant "engaged in a pattern of methodically seeking out child pornography, by conducting image searches for terms . . . [associated with child pornography] and downloading websites consistent with child pornography." *Id*. at 1203. The Tenth Circuit concluded that this evidence of knowledge was insufficient to establish

a conviction for receipt. It focused on the fact that "there was no evidence that [the defendant] even knew about his computer's automatic-caching function," nor was there evidence that he "even saw" the images in question. *Id*. at 1204.

Dobbs, of course, is not binding on us.[5] Even so, Fall's illicit conduct here is more extensive than the conduct in *Dobbs*. The forensic examiner in *Dobbs* "discovered over 150 images of child pornography in the hard drive's temporary Internet files folder." *Id*. at 1201. The defendant's conduct in that case involved a single device and occurred over a period of only six months. *Id*. at 1211. By contrast, the record here contained evidence of over ten years of illicit conduct across multiple devices and thousands of images and videos of child pornography.

[5] And to the extent we have considered *Dobbs* in the past, our previous interpretations of it support the government's position. We first looked to *Dobbs* in *United States v. Johnson*, 523 F. App'x 219 (4th Cir. 2013). There, we cited *Dobbs* for limited assertion that "[i]f, for example, the evidence shows only that the images were saved to the computer's cache or temporary internet folders and that the defendant made no effort to remove them, or that the images were otherwise saved automatically to locations inaccessible to a computer user, there may be some reason to believe that the defendant did not 'knowingly' receive the images." *Id*. at 222. We then distinguished that case from *Dobbs* by noting that, among other factors, the defendant had repeatedly sought child pornography online and stored it in a Word document. *Id*. at 223. Similarly, Fall repeatedly sought child pornography and created a folder on the roof laptop, which he filled with images of child pornography.

We also cited *Dobbs* in *United States v. Myers*, 560 F. App'x 184 (4th Cir. 2014). There, too, we affirmed a conviction for receiving child pornography based on "circumstantial evidence of knowledge." *Id*. at 187. We explained that "investigators discovered a plethora of child pornography on [the defendant's] computer, thus establishing that it was not by mistake or error that the files were downloaded." *Id*. Under these cases, it was reasonable for the jury to conclude that Fall did not stumble upon the child pornography that formed the basis of his receipt charge.

Upon reviewing the record, we believe that the evidence adequately supports the jury's conclusion that Fall knowingly received the three images charged in Counts 3 through 5. Our standard of review is important to this conclusion. It requires us to view the evidence in the light most favorable to the government. And it requires us to affirm the jury's verdict if any trier of fact could have found that the evidence—either direct, circumstantial or a combination of both—along with any reasonable inference, established that Fall knowingly received child pornography. Here, there was ample evidence from which a reasonable jury could have found Fall guilty on Counts 3 through 5. Therefore, we affirm the district court.

VI.

For these reasons, the judgment of the district court is

AFFIRMED.