

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

August Term 2017

(Argued: April 16, 2018

Decided: January 25, 2019)

Docket No. 17-1138-cr

UNITED STATES OF AMERICA,
Appellee,

- *against* -

DONALD RAY BOLES,
Defendant-Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF VERMONT

Before:

WESLEY, CHIN, AND CARNEY, *Circuit Judges.*

Appeal from a judgment of the United States District Court for the District of Vermont (Sessions, *J.*) convicting defendant-appellant, following a jury trial, of one count of possessing child pornography and sentencing him principally to 120 months' imprisonment followed by ten years' supervised

release. On appeal, defendant-appellant raises three principal challenges: (1) the district court erred in denying his motion to suppress evidence of child pornography seized at his home pursuant to a search warrant; (2) the government failed at trial to prove that computers seized at his home had been transported in interstate or foreign commerce or had been used to produce child pornography; and (3) the district court erred in sentencing him to a mandatory minimum term of imprisonment and in imposing two special conditions of supervised release.

AFFIRMED IN PART, VACATED IN PART, AND REMANDED.

BARBARA A. MASTERSON, Assistant United States Attorney (Gregory L. Waples, Assistant United States Attorney, *on the brief*), for Christina E. Nolan, United States Attorney for the District of Vermont, Burlington, Vermont, *for Appellee*.

STEVEN L. BARTH, Assistant Federal Public Defender (Barclay T. Johnson, Assistant Federal Public Defender, *on the brief*), for Michael L. Desautels, Federal Public Defender for the District of Vermont, Burlington, Vermont, *for Defendant-Appellant*.

CHIN, *Circuit Judge*:

In this case, defendant-appellant Donald Ray Boles was convicted in the United States District Court for the District of Vermont, following a jury trial, of possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). On April 17, 2017, the district court sentenced him principally to 120 months' incarceration and a ten-year term of supervised release. On appeal, he contends that the district court erred in denying his motion to suppress evidence obtained in a search of his home pursuant to a warrant. He raises other issues relating to his trial and sentence. We affirm the conviction and sentence, except that we vacate the "risk" condition of his supervised release and remand in that respect only.

BACKGROUND

A. *The Facts*¹

In 2001, in an earlier case, Boles pleaded guilty to possession of child pornography, also in the U.S. District Court for the District of Vermont. The court (Sessions, J.) sentenced him to 15 months in prison and two years'

¹ The facts herein are drawn from the affidavit that supported the warrant for Boles's arrest, J. App. 40-66.

supervised release. Boles served his prison term and completed his supervised release on August 8, 2004.

In January 2010, the Innocent Images Operations Unit (the "IIOU") of the Federal Bureau of Investigation (the "FBI") investigated the distribution of child pornography via an online message board called "Girls.Forumcircle.com." The IIOU investigation revealed that the message board was password-protected, had around 65 members, and was utilized to trade both illegal child pornography and legal "child erotica" (images of children that are not sexually explicit but that may be "sexually arousing to a given individual," *see United States v. Martin*, 426 F.3d 68, 79 (2d. Cir. 2005)). The investigation further revealed that a user named "drb05" was a member of Girls.Forumcircle.com and was linked to the email address "drb0505@hotmail.com."

Between August and November 2009, the administrator of Girls.Forumcircle.com posted messages that users' accounts would be deleted if they did not post photos or videos on the forum by November 30. On November 30, 2009, user drb05 posted 13 images of child erotica (not child pornography) depicting a young girl in sexually suggestive poses. User drb05 also posted two comments on the message board indicating a sexual interest in young girls: one

in response to other users' posts of child erotica on November 29 and one accompanying drb05's post of child erotica on November 30.

On July 19, 2010, the IIOU served a subpoena on Microsoft. The responsive materials revealed that "drb0505@hotmail.com" was associated with a "Don B" in "Vermont, 05301." The materials also revealed a log of IP addresses for recent logins for drb0505@hotmail.com. On August 4, 2010, the IIOU subpoenaed internet service provider FairPoint Communications ("FairPoint") requesting information about subscribers associated with the IP addresses obtained from Microsoft, but FairPoint responded that it could not link IP addresses to specific subscribers.

During its investigation, the IIOU also operated an FBI undercover website that advertised access to free child pornography. The "home page" of the website made clear that its purpose was to share child pornography. The home page also contained a login field that required a unique password to access the rest of the website. Users obtained unique passwords by responding to a personal email advertisement sent undercover by the FBI. Once a user entered the unique password, the user was taken to the "landing page," which listed and described free child pornography videos available to view or download. When a

user clicked on the "download" button for any of these videos, the website recorded the user's IP address, video sample number, and the number of downloads attempted, but no child pornography was actually made available. The landing page also included a link to a "paid area," where users could ostensibly pay to view a live stream of child pornography from Eastern Europe.

On September 2, 2010, the FBI sent such an email to drb0505@hotmail.com. On September 6, 2010, a user from IP address 72.92.136.14 accessed the home page of the undercover website and entered the unique password sent to drb0505@hotmail.com. After arriving at the landing page, however, this user did not attempt to view or download any of the advertised child pornography videos or access the "paid area" of the undercover website. At some point after sending the first email, an agent sent a new email to drb0505@hotmail.com, but the user did not respond. Using this information, the IIOU again served a subpoena upon FairPoint requesting the information of any subscribers associated with the IP address 72.92.136.14, but FairPoint again stated that it could not link subscribers to IP addresses.

Nearly one year later, on July 21, 2011, FBI Special Agent Jeffrey Alford sent an email to FBI Special Agent Christopher Hughes regarding an

application for a warrant to search Boles's residence, as Boles was the suspected owner of drb0505@hotmail.com. In this email, Alford asked whether there had been recent efforts to reach out to Boles regarding the undercover website, acknowledging that "I might otherwise now have a 'staleness' issue." J. App. 67. Hughes responded that he had sent a new email but "[Boles] did not respond to the new request -- there may be a staleness issue with this at this point but it's worth seeing if the AUSA will go for it." J. App. 69. On August 19, 2011, the agents confirmed from a subpoena served upon eBay that drb0505@hotmail was operated by Boles, and the subpoena also revealed Boles's home address.

On August 25, 2011, the agents applied for a warrant to search and seize computer evidence from Boles's residence. The district court (Sessions, J.) issued the warrant the same day, finding that probable cause supported the request. The agents executed the warrant on September 6, 2011. More than 100 images of child pornography were discovered on Boles's computer and hard drives.

B. *Proceedings Below*

On July 15, 2014, Boles was charged with possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). He was ultimately tried on

a second superseding indictment (the "Indictment") that charged three counts: one count of possessing child pornography and two counts of access with intent to view child pornography, all in violation of 18 U.S.C. § 2252(a)(4)(B).

On December 22, 2014, Boles moved to suppress the seized evidence on the basis that the warrant was not supported by probable cause and the information in the affidavit was stale when the warrant was issued. The district court denied Boles's motion in a written decision filed April 2, 2015.²

Trial commenced on May 31, 2016. The district court received into evidence, over Boles's objection, two computers (with hard drives inside) and a separate hard drive seized at Boles's residence pursuant to the warrant. Labels affixed to the computers and hard drives identified the manufacturer and showed the place of origin as being outside the United States (China and Thailand). Boles argued that the labels were hearsay. The district court overruled the objection and admitted the computer evidence. The district court also permitted an FBI agent to testify, again over defense counsel's objection, that the types of computer hardware in question (Hitachi, Compaq, and Hewlett Packard) were manufactured outside the United States. On June 3, 2016, the jury

² In its opinion, the district court noted that it was "in the somewhat unusual position of reviewing a warrant that it issued in the first place." J. App. 97.

convicted Boles on the possession count but acquitted him on the two access charges.

Prior to sentencing, Boles objected to several conditions of supervised release proposed in his PSR, including two at issue on this appeal: (1) the "risk" condition, which requires Boles to notify any person or organization of any risk he posed if his probation officer determined Boles was a risk; and (2) the "polygraph" condition, which requires Boles to submit to a polygraph exam as directed by the probation officer as part of his sex offender treatment program. At sentencing on April 17, 2017, the district court overruled Boles's objections to the conditions. The district court sentenced Boles to 120 months' imprisonment -- the mandatory minimum -- and ten years' supervised release, imposing the disputed conditions.

This appeal followed.

DISCUSSION

On appeal, Boles raises three principal challenges: (1) the district court erred in denying his motion to suppress because the search warrant issued without probable cause; (2) the government failed at trial to sufficiently prove the interstate or foreign commerce element of the crime of conviction; and (3) the

district court erred in sentencing him to a mandatory minimum term of imprisonment and in imposing the two disputed conditions of supervised release. We discuss each challenge in turn.

I. *The Motion to Suppress*

Boles argues that the warrant to search his residence was not supported by probable cause because the affidavit submitted in support of the request for the warrant alleged nothing more than legal activity and was based on stale information. The government contends, however, that the district court did not err in finding probable cause because the record established that Boles was a collector of child pornography who likely was hoarding such images. Moreover, the government argues that, even assuming the warrant issued without probable cause, the district court did not err in denying the motion based on the good faith exception to the exclusionary rule.

We do not decide whether probable cause existed to support the issuance of the warrant, for we agree that in the circumstances here, even assuming the warrant was not supported by probable cause, the good faith exception applies.

A. *Applicable Law*

The Fourth Amendment prohibits "unreasonable searches and seizures" and provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation." U.S. Const. amend. IV.

In determining whether probable cause exists to support the issuance of a warrant, a judge must "make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *United States v. Falso*, 544 F.3d 110, 117 (2d Cir. 2008) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)) (alteration in original). "On appeal from a district court's ruling on a motion to suppress, we review the court's factual findings for clear error. We review the court's legal determinations, including the existence of probable cause and the good faith of officers relying on a search warrant, *de novo*." *United States v. Raymonda*, 780 F.3d 105, 113 (2d Cir. 2015) (citation omitted). We accord "'substantial deference to the finding of an issuing judicial officer that probable cause exists,' limiting our inquiry to whether the officer 'had a substantial basis' for his determination." *Id.* (quoting *United States v. Wagner*, 989 F.2d 69, 72 (2d Cir. 1993)).

Even where a warrant was issued without probable cause in violation of the Fourth Amendment, suppression of the evidence is not automatic; rather, because the remedy exacts a heavy toll on the justice system, the exclusionary rule will apply only to deter "deliberate, reckless, or grossly negligent conduct" by law enforcement. *Herring v. United States*, 555 U.S. 135, 144 (2009). Accordingly, "[w]hen an officer genuinely believes that he has obtained a valid warrant . . . and executes that warrant in good faith, there is no conscious violation of the Fourth Amendment, 'and thus nothing to deter.'" *Raymonda*, 780 F.3d at 118 (quoting *United States v. Leon*, 468 U.S. 897, 921 (1984)); see also *Falso*, 544 F.3d at 125 (explaining that evidence obtained by officers "in objectively reasonable reliance" on a subsequently invalidated warrant is not generally subject to exclusion).

For an officer to be able to claim the benefits of the good faith exception, however, his reliance on a warrant must be objectively reasonable. See *Leon*, 468 U.S. at 922. Thus,

the good faith exception cannot shield [] an officer who relies on a duly issued warrant in at least four circumstances: (1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so

lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable.

Raymonda, 780 F.3d at 118 (quoting *United States v. Clark*, 638 F.3d 89, 100 (2d Cir. 2011); see also *Leon*, 468 U.S. at 923 (suppression is an appropriate remedy if the magistrate issuing the warrant 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"). "When the police exhibit 'deliberate,' 'reckless,' or 'grossly negligent' disregard for Fourth Amendment rights, the deterrent value of exclusion is strong and tends to outweigh the resulting costs" of suppression. *Davis v. United States*, 564 U.S. 229, 238 (2011) (internal quotation marks omitted).

B. *Application*

The existence of probable cause in this case presents a close question. We need not decide the issue, however, because we conclude that, even assuming probable cause was lacking, the good faith exception applies. The government argues that even if the warrant to search Boles's residence was not supported by probable cause, the FBI agents were justified in relying on the district court's determination that the warrant was valid. We agree.

In *Raymonda*, we directly addressed the exclusionary rule in the context of an affidavit containing potentially stale and misleading information. In that case, the affidavit supporting the warrant application alleged only that, on one occasion nine months earlier, a user with an IP address associated with Raymonda's home opened between one and three pages of a website housing thumbnail links to images of child pornography but did not click on any thumbnails to view full-sized files. 780 F.3d at 117. The affidavit was written as to suggest that the suspect intentionally accessed 76 pornographic images, and, significantly, it omitted the fact that the images were open for just seventeen seconds, a time span consistent with a user having "simply closed" the site immediately after clicking on it, rather than intentionally saving or viewing all of the images that his browser had accessed. *Id.* at 111-12.

Absent any further indicia that Raymonda was a collector of child pornography, we concluded that the single incident of access, which was "at least equally consistent with an innocent user inadvertently stumbling upon a child pornography website," did not create a fair probability that child pornography would be found on Raymonda's computer months later. *Id.* at 117. We therefore agreed with the district court that the warrant lacked probable cause. We

reversed, however, the district court's grant of Raymonda's motion to suppress the evidence, holding that the agents who had executed the search were entitled to rely in good faith on the duly issued warrant for two reasons: (1) the magistrate judge had reached an independent determination of probable cause that, while ultimately incorrect, was not contrary to established law or so facially deficient that reliance upon it would be unreasonable, and (2) we disagreed with the district court that an agent had acted in such a "grossly negligent" manner with respect to the warrant application as to justify exclusion of the evidence. *See id.* at 121.

In concluding that the agent had not been grossly negligent, first, we disagreed with the district court that the agent was effectively on notice about a staleness issue with the nine-month old evidence because he had previously worked on a case in which one-year-old evidence was found to be stale. *Id.* at 119. We explained that the agent's knowledge that an earlier case found nearly year-old evidence too stale to create probable cause could not have given him sufficient notice that his affidavit in *Raymonda* would be found equally deficient. *See id.* ("[A prior holding by a district court cannot establish a binding principle of law sufficient to undermine an agent's good faith reliance on a later warrant.]).

Second, we rejected the argument that there were key omissions and exaggerations in the affidavit that had materially misled the magistrate judge issuing the warrant. Although we acknowledged that the agent "may have exaggerated the significance of" certain facts and potentially "mischaracteriz[ed]" the evidence, we nevertheless determined that, absent a finding that the agent intended to deceive the magistrate judge with these statements, the "oversights" fell "short of deliberate deception or gross negligence." *Id.* at 120. We therefore held that agents were entitled to rely in good faith on the warrant. *See id.* at 121.

As in *Raymonda*, the agents in this case were entitled to rely in good faith on the duly issued warrant. First, the district court made an independent determination that the warrant was supported by probable cause, which it based primarily on: (1) Boles's membership in Girls.Forumcircle.com and his postings of child erotica; (2) Boles's visit to the FBI Undercover website using the unique code that was emailed to him; and (3) Boles's prior conviction for possession of child pornography. Even assuming that these facts did not add up to probable cause, the existence of probable cause in this case is an exceedingly close question. Accordingly, the court's finding of probable cause was not facially

insufficient such that any reliance upon the warrant would be unreasonable. *Id.* at 121.

Second, as in *Raymonda*, the representations in the affidavit here were not intentionally false, reckless, or grossly negligent such as to otherwise preclude the good faith exception. Boles attempts to distinguish this case from *Raymonda* on the ground that here the agents were specifically aware that "there may be a staleness issue with [the evidence]" prior to applying for the warrant. We are not persuaded, however, that the agents acted in reckless disregard of Boles's Fourth Amendment rights merely because they knew of a possible staleness issue before applying for the warrant. As the district court noted, the exchange does indicate "some degree of uncertainty on the part of the agents" as to whether the evidence would be considered stale. Sp. App. 15. But there was nothing inappropriate in their leaving the issue to the prosecutor and court to resolve. As this Court has repeatedly recognized, there is "no bright-line rule for staleness," *Walczyk v. Rio*, 496 F.3d 139, 162 (2d Cir. 2007), which depends "on the basis of the facts of each case," *United States v. Martino*, 664 F.2d 860, 867 (2d Cir.

1981); accord *Raymonda*, 780 F.3d at 114. While some of the information here arguably was stale, other facts weighed against a finding of staleness.³

Even assuming the information was stale, the agents disclosed the information to a neutral and detached judge, who was made aware of the "staleness issue" and the relevant facts and circumstances, but nevertheless issued the warrant. The agents cannot be said to have acted in bad faith by asking a judge to decide the question of staleness. See *Leon*, 468 U.S. at 922 (evidence seized "in objectively reasonable reliance on" warrant issued by detached and neutral judge is admissible, even where reviewing court later determines warrant was invalid).

³ For example, (1) Boles had previously been convicted of possession of child pornography in June 2000, see *Raymonda*, 780 F.3d at 114 (evidence that "persons possessed child pornography in the past supports a reasonable inference that they retain those images -- or have obtained new ones -- in the present"); (2) Boles apparently had joined Girls.Forumcircle.com, a website used for posting and trading illegal child pornography and legal erotica, see *Martin*, 426 F.3d at 73 (upholding warrant to search defendant's computer where he had recently joined an Internet group devoted to distributing child pornography, even absent evidence that he had actually accessed any illicit images through that site); and (3) Boles had entered a unique code enabling him to access the FBI undercover page, which advertised its purpose as the distribution of child pornography, see *United States v. Vosburg*, 602 F.3d 512, 517 (3d Cir. 2010) (no staleness where suspect had to enter decoded URL and could not access images of child pornography "with a simple click of the mouse").

Finally, we note that the affidavit in this case disclosed that Boles had not attempted to download child pornography from the FBI undercover website and that he had not responded to the FBI's second email solicitation. Hence, the agents disclosed these facts to the district court, and the district court noted these facts in nonetheless denying the motion. While the agents here arguably should have provided more information, including, for example, details relating to the Girls.Forumcircle.com website, any omissions and exaggerations were not as egregious as those in *Raymonda*, where we held that the good faith exception applied even though there were at least arguable omissions and exaggerations in the agent's affidavit. *See* 780 F.3d at 122 (Chin, J., dissenting). We are hard-pressed to conclude that the agents acted in a deliberate or reckless or grossly negligent manner here.

We therefore agree with the district court that, despite the agents' uncertainty as to whether the evidence was stale, "[o]nce the Court ruled on the legal sufficiency of the facts alleged in the affidavit, the officers were justified in" subsequently relying on that determination and executing the warrant. *See* Sp. App. 16; *see also Herring*, 555 U.S. at 144. We conclude that the district court did not err in denying Boles's motion to suppress the computer evidence.

II. *The Interstate or Foreign Commerce Requirement*

Boles makes three arguments with respect to the interstate or foreign commerce element of the crime of conviction: (a) the government constructively amended the Indictment in its proof at trial; (b) the government failed to present sufficient evidence that the images on his computer were "produced" using materials transported by a means of interstate or foreign commerce; and (c) the district court erred in admitting evidence that the computers and hard drives were manufactured outside the United States.

A. *Constructive Amendment*

Boles argues that the government constructively amended the Indictment charging him with one count of possession of child pornography under 18 U.S.C. § 2252(a)(4)(B).⁴ The Indictment alleged that Boles

⁴ The statute provides in relevant part:

Any person who . . . knowingly possesses, or knowingly accesses with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if -- (i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (ii) such visual depiction is of such conduct; . . . [commits a crime].

18 U.S.C. § 2252(a)(4)(B).

possessed at least one matter which contained a visual depiction that was produced using materials which had been mailed and shipped and transported *using any means and facility of interstate and foreign commerce, including by computer, the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct, and such visual depiction was of such conduct.*

J. App. 15 (emphasis added). Boles argues that, as written, the Indictment required the government "to prove that the computer hardware was mailed, shipped, or transported 'using' a '*means and facility of interstate or foreign commerce.*'" Def.-Appellant's Reply Br. 15 (emphasis in original). The district court charged the jury, however, that it had to find only "that the visual depiction was produced using materials that had been *transported in or affecting interstate or foreign commerce.*" J. App. 271. Boles contends that the government failed to prove the actual means by which the hardware had traveled.

1. *Applicable Law*

We review a constructive amendment challenge *de novo*. See *United States v. Agrawal*, 726 F.3d 235, 259 (2d Cir. 2013). To prevail on a constructive amendment claim, a defendant must establish that "the terms of the indictment are in effect altered by the presentation of evidence and jury instructions which so modify *essential elements* of the offense charged that there is a substantial

likelihood that the defendant may have been convicted of an offense other than that charged in the indictment." *United States v. D'Amelio*, 683 F.3d 412, 416 (2d Cir. 2012) (internal quotation marks omitted) (emphasis in original); *see also United States v. Spoor*, 904 F.3d 141, 152 (2d Cir. 2018).

Where a defendant fails to raise a claim in the district court, we must also review for plain error to assess the impact of any alleged error on the defendant's rights. *United States v. Taylor*, 816 F.3d 12, 18 (2d Cir. 2016). To establish plain error, a defendant must demonstrate "(1) error, (2) that is plain, and (3) that affect[s] substantial rights. If all three conditions are met, an appellate court may then exercise its discretion to notice a forfeited error, but only if (4) the error seriously affect[s] the fairness, integrity, or public reputation of judicial proceedings." *Id.* (brackets in original) (quoting *Johnson v. United States*, 520 U.S. 461, 467 (1997)).

2. Application

Boles argues that, under the Indictment as written, the government was required to present evidence of the actual *means* or *facility* by which the computer hardware traveled interstate. We conclude that the district court did not plainly err in charging the jury that it only had to find that the hardware had

been transported in or affected interstate commerce. Boles did not raise this issue below, and, as did the government, proceeded on the basis that the government was required only to prove that the computer hardware traveled *in* interstate commerce, not the actual means by which it had traveled.

Furthermore, in discussions with the district court about the jury charge, defense counsel specifically requested that the jurors not see the actual Indictment because he did not want them "focused" on it. Boles was therefore adequately informed about the arguments the government intended to make about the jurisdictional element and the types of evidence it would produce to support its theory. Thus, there was no error, much less error that was "plain."

Moreover, for purposes of plain error review, we do not view as significant the difference between proving (a) the "means or facility" of interstate travel (that is, how the equipment was physically transported) and (b) the fact that the equipment was shipped or transported in interstate or foreign commerce. *See* 18 U.S.C. § 2252(a)(4)(B) (referring to any matter containing "any visual depiction that has been . . . shipped or transported using any means or facility of interstate or foreign commerce" or "produced using materials which have been mailed or so shipped or transported, by any means").

Finally, we have held that there is sufficient evidence to support conviction for possession of child pornography where a defendant possessed images of child pornography on computer equipment manufactured outside this country. *See United States v. Ramos*, 685 F.3d 120, 132-33 (2d Cir. 2012) (applying interstate commerce element of § 2252A(a)(5)(B)); *accord United States v. Grzybowicz*, 747 F.3d 1296, 1306-07 (11th Cir. 2014); *United States v. Anderson*, 280 F.3d 1121, 1125 (7th Cir. 2002). Accordingly, we are not persuaded that the error "affect[ed] the fairness, integrity, or public reputation of judicial proceedings." *Johnson*, 520 U.S. at 467 (internal quotation marks omitted).

B. *The Evidence of "Production"*

Boles further argues that the government failed to prove that the hardware was used to "produce" the child pornography because the government did not present evidence that the seized hardware was used to create the child pornography in the first instance (*i.e.*, that Boles had manufactured the child pornography *using* the hardware rather than merely storing copies of the images on the hardware).

This Court has not specifically addressed the question of whether merely transferring or copying child pornography using materials that have

traveled interstate means that the child pornography has been "produced" using those materials as required under 18 U.S.C. § 2552(a)(4)(B). *See Ramos*, 685 F.3d at 133 n.10 (explaining that the court would not reach the question of whether "the mere copying or downloading of an image is 'production' for purposes of the federal child pornography statutes").⁵

Almost every circuit to address this issue, however, has held that the word "produced" encompasses mere copying or downloading of child pornography. *See United States v. Burdulis*, 753 F.3d 255, 262 (1st Cir. 2014) (images are "produced" for the purposes of § 2254(a)(4)(B) when they are copied or downloaded onto a digital medium); *United States v. Dickson*, 632 F.3d 186, 189-90 (5th Cir. 2011) (same); *United States v. Angle*, 234 F.3d 326, 341 (7th Cir. 2000) (same); *United States v. Lacy*, 119 F.3d 742, 750 (9th Cir. 1997) (same). *But see United States v. Wilson*, 182 F.3d 737, 742-43 (10th Cir. 1999) (holding that the

⁵ Although the government argues that we decided this issue in *United States v. Pattee*, 820 F.3d 496 (2d Cir. 2016), there we interpreted "production" in the context of 18 U.S.C. § 2251, rather than the statute at issue here, 18 U.S.C. § 2252(a)(4)(B). Moreover, we noted that

[i]t does not follow from this conclusion, however, that merely transferring or copying a pornographic image that was produced by someone else is tantamount to "producing" child pornography, such that simple possession, which typically involves making a copy of a file to a hard disk or other medium, would qualify as production.

Id. at 511 n.8.

government produced insufficient evidence to support the interstate commerce element of § 2252(a)(4)(B) because there was no evidence that the digital mediums were used to produce the graphic files even though the files could be stored on the mediums).

Those circuits that have interpreted "produced" to include copying or transferring rely on 18 U.S.C. § 2256(3), which defines the word "producing" in the child pornography and child exploitation statutes to mean "producing, directing, manufacturing, issuing, publishing, or advertising." 18 U.S.C. § 2256(3); *see also Angle*, 234 F.3d at 341. The plain meaning of the word "produced" would include producing or making a copy. Moreover, we agree that to interpret "produced" to exclude pulling up images on a computer monitor is "far too restrictive as it essentially renders meaningless the statutory definition of 'producing' [in § 2256(3)] . . . and focuses entirely on the circumstances surrounding the original or actual production of the visual depiction." *Angle*, 234 F.3d at 241. To read the statute this way would require the government to present evidence about the *original* materials used to create the child pornography in every case a defendant is charged under the "produced using materials" language. Boles fails to point to, and we are unable to find, any

evidence that Congress intended these subsections to be applied so narrowly. Indeed, the nature of the industry is that these images are copied over and over again as collectors share them, and it would be difficult in many cases to prove the circumstances of the original "production."

Therefore, we agree that the government was not required to prove that the hardware was used to create the pornography in the first instance and that it was sufficient for the government to prove that the hardware was used to make, store, or display copies of the pornographic images.

C. *The Evidence the Computer Equipment Was Manufactured Outside the United States*

Boles argues that the district court erred by (1) admitting inscriptions on the back of seized pieces of computer hardware because the labels were inadmissible hearsay; and (2) allowing Agent Alfin to testify as an expert about where the relevant companies manufacture hardware.

A district court has "broad discretion" over the admission of evidence. *United States v. Nektalov*, 461 F.3d 309, 318 (2d Cir. 2006). Accordingly, "[t]his [C]ourt reviews evidentiary rulings for abuse of discretion." *United States v. Cummings*, 858 F.3d 763, 771 (2d Cir. 2017). "A district court has abused its discretion if it based its ruling on an erroneous view of the law or on a clearly

erroneous assessment of the evidence or rendered a decision that cannot be located within the range of permissible decisions." *United States v. Natal*, 849 F.3d 530, 534 (2d Cir. 2017) (per curiam) (internal quotation marks omitted).

1. *The Hardware Inscriptions*

We have not directly addressed whether manufacturers' inscriptions or labels identifying a product's country of origin are inadmissible hearsay. We conclude that the district court did not abuse its discretion in allowing evidence of the inscriptions here.

As a threshold matter, there is some doubt as to whether the inscriptions are hearsay at all, as the government, relying principally on gun cases, argues that under the "mechanical trace" theory, markings on products designating country of origin are not "statements" subject to the hearsay rule. *See* Fed. R. Civ. P. 801(a), (c); *United States v. Bowling*, 32 F.3d 326, 328 (8th Cir. 1994) (holding that manufacturer's name stamped on firearm was not "a statement of fact" subject to hearsay rule); *United States v. Thody*, 978 F.2d 625, 630-31 (10th Cir. 1992) ("[T]he manufacturer's imprint in the gun is not hearsay. It is technically not an assertion by a declarant as contemplated by the [hearsay rule]."); *United States v. Alvarez*, 972 F.2d 1000, 1004 (9th Cir. 1992) ("An inscription placed on a

firearm by the manufacturer is similarly a mechanical trace and not a statement for purposes of Federal Rule of Evidence 801(c)."), *overruled on other grounds by Kawashima v. Mukasey*, 530 F.3d 1111, 1116 (9th Cir. 2008). We need not decide the issue because, even assuming the inscriptions here are hearsay, we conclude that they are nonetheless admissible.

Inscriptions indicating foreign origin are regulated, *see* 19 U.S.C. § 1304, and federal law prohibits misleading designations of origin, *see* 15 U.S.C. § 1405. Additionally, under Federal Rule of Evidence 902(7), trade inscriptions are self-authenticating, that is, they "require no extrinsic evidence of authenticity in order to be admitted." Fed. R. Evid. 902. While Boles is correct that self-authentication alone does not qualify as an exception to the hearsay rule, it does render the inscriptions particularly trustworthy. As the First Circuit has noted, "[a]n authentic inscription, of the kind made regularly by manufacturers in accordance with federal law, bears significant similarity to other forms of evidence admissible under the enumerated hearsay exceptions." *Burdulis*, 753 F.3d at 263-64 (citing Fed. R. Evid. 803(6) (records of regularly conducted activity), 803(9) (certain information reported to a public office in accordance with a legal duty), and 807 (residual exception)); *accord United States v. Koch*, 625

F.3d 470, 480 (8th Cir. 2010) (rejecting claim that "manufacturer's inscription on a product is inadmissible hearsay"). Any of these exceptions would suffice here, and we hold that the district court did not abuse its discretion in overruling the hearsay objection.

2. *The Agent's Testimony as an Expert*

Boles also argues that the district court erred by permitting FBI Special Agent Alfin to testify about the origin of the computer hardware. Rule 702 permits testimony in the form of an opinion only if "the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue." Fed. R. Evid. 702(a). Boles additionally argues that the defense had been given no prior notice in the government's Rule 16 expert disclosure that Alfin would testify about the manufacturing origin of the hardware.

A district court has "broad discretion" in deciding whether to admit expert testimony, and the exercise of that discretion will not be disturbed unless it is "manifestly erroneous." *United States v. Locasio*, 6 F.3d 924, 936 (2d Cir. 1993); accord *United States v. Dukagjini*, 326 F.3d 45, 52 (2d Cir. 2003). We discern no manifest error here, where the district court permitted an FBI agent with

specialized training and experience in computers, computer forensics, and forensic imaging to testify that he knew the computer hardware in question was manufactured outside Vermont and outside the United States.

While there is a dispute as to whether the government provided sufficient notice of the agent's testimony as an expert as required by Fed. R. Crim. P. 16(a), even assuming the testimony was not properly noticed, the district court had the discretion to admit the evidence nonetheless as long as the violation did not cause Boles "substantial prejudice." *United States v. Thai*, 29 F.3d 785, 804 (2d Cir. 1994). Here, Boles has not identified any prejudice from the purported lack of advance notice, and the record is clear in any event that Boles and his counsel knew that the government intended to introduce evidence to prove the interstate or foreign commerce nexus. Finally, as we have held that the manufacturers' inscriptions were admissible, any error with respect to the admission of the agent's testimony in this respect was harmless.

III. *The Sentence*

Boles raises two challenges to his sentence: (a) the imposition of the mandatory minimum term of imprisonment; and (b) the imposition of the two disputed special conditions of supervised release.

A. *The Mandatory Minimum*

First, Boles argues that the district court's application of the ten-year mandatory minimum penalty, under 18 U.S.C. § 2252(b)(2), violated the Sixth Amendment because Boles's prior conviction was not found by the jury beyond a reasonable doubt. His argument, however, is expressly foreclosed by this Court's decision in *United States v. Arline*, 835 F.3d 277 (2d Cir. 2016) (per curiam), where we acknowledged that "[t]he fact of a prior conviction may be decided by a judge and need not be determined by a jury." *Id.* at 280 (citation omitted). Accordingly, the district court properly recognized that the mandatory minimum of ten years applied to Boles.

B. *The Conditions of Supervised Release*

Second, Boles raises challenges to two conditions of his supervised release. He challenges Standard Condition 17, the "risk" condition, which provides:

If the probation officer determines that you pose a risk to another person (including an organization), the probation officer may require you to notify the person about the risk and you must comply with that instruction. The probation officer may contact the person and confirm that you have notified the person about the risk.

PSR ¶ 95, Cond. 27.

Boles specifically argues that the risk condition is "far too vague to be related to any goal of supervision" because the court did not define "risk," and the condition leaves "too much discretion[] to the supervising officer." Def.-Appellant's Br. 14-15.

Boles also challenges the "polygraph" condition of supervised release, which provides that Boles:

shall participate in an approved program of sex offender evaluation and treatment, which may include polygraph examinations, as directed by the probation officer. Any refusal to submit to such assessment or tests as scheduled is a violation of the conditions of supervision.

PSR ¶ 96, Cond. (a).

Boles contends that the condition violates the Fifth Amendment, because if he answers questions, he may incriminate himself, and on the other hand, if he invokes his Fifth Amendment right to remain silent, he violates the condition, and will be subject to having his supervised release revoked.

1. *Applicable Law*

We generally review the imposition of conditions of supervised release for abuse of discretion. *See United States v. Reeves*, 591 F.3d 77, 80 (2d Cir. 2010). "When a challenge to a condition of supervised release presents an issue

of law," however, "we review the imposition of that condition *de novo*, bearing in mind that any error of law necessarily constitutes an abuse of discretion." *United States v. McLaurin*, 731 F.3d 258, 261 (2d Cir. 2013) (internal quotation marks omitted).

A district court may

impose special conditions of supervised release to the extent that they are reasonably related to (i) the nature and circumstances of the offense and the history and characteristics of the defendant, and (ii) the purposes of sentencing, including the need to afford adequate deterrence, to protect the public from further crimes of the defendant, and to provide the defendant with needed training or treatment.

United States v. Johnson, 446 F.3d 272, 277 (2d Cir. 2006) (quoting *United States v.*

Germosen, 139 F.3d 120, 131 (2d Cir. 1998)); *see also* 18 U.S.C. § 3583(d). "While

district courts have broad discretion to tailor conditions of supervised release,

that discretion is not unfettered," and we will "carefully scrutinize conditions that

may be excessively harsh or inexplicably punitive." *United States v. Jenkins*, 854

F.3d 181, 188 (2d Cir. 2017) (internal citations omitted).

2. Application

As to the first challenged condition, we agree with Boles that the

"risk" condition is vague and affords too much discretion to the probation officer.

In *United States v. Peterson*, we vacated a district court's imposition of two similar standard conditions of supervised release, in part, because they, too, gave the probation officer too much discretion. 248 F.3d 79, 86 (2d Cir. 2001) (per curiam). The defendant in *Peterson* was convicted of bank larceny, but the court noted that the supervised release conditions were "based in part on a prior, unrelated New York state-sex-offense conviction [for incest]." *Id.* at 81.

In *Peterson*, we held that the conditions were impermissible to the extent that they required Peterson to notify employers about his state conviction, because occupational restrictions must be related to the offense of conviction at issue. *Id.* at 85-86. We further held, to the extent that the conditions required Peterson to notify employers about his federal conviction, "the [district] court must determine, rather than leaving to the discretion of the probation officer, whether such notification is required . . . [and] may not simply leave the issues of employer notification to the probation officer's unfettered discretion." *Id.* at 86. We therefore remanded the case for clarification of the nature and scope of employer notification of the offense of conviction. *Id.*

Because the condition at issue here extends to warning employers of risk and gives the probation office unfettered discretion with respect to the

notification requirement, we agree with Boles that the condition is largely indistinguishable from the one we struck down in *Peterson*. Accordingly, we vacate the risk condition and remand to the district court to clarify the scope of the "risk" condition.

We are not persuaded, however, as to Boles's challenge to the polygraph condition of supervised release. In *Johnson*, 446 F.3d at 272, we upheld a polygraph condition against a Fifth Amendment challenge, similar to the one at issue here. We held that requiring a defendant to take a polygraph test as a condition of his supervised release does not violate the Fifth Amendment because the defendant retains the right to later challenge any resulting self-incrimination in court. *Id.* at 280; *see also Asherman v. Meachum*, 957 F.2d 978, 982-83 (2d Cir. 1992) (en banc) (explaining that revocation may be based on a refusal to answer questions, so long as the administrator does nothing to impair later invocation of the Fifth Amendment privilege).

Furthermore, in upholding the condition in *Johnson*, we recognized the strong deterrent value of polygraph conditions, explaining that such conditions "further sentencing objectives such as rehabilitation and deterrence, with reasonably small incremental deprivations of liberty." *Johnson*, 446 F.3d at

278. When the district court imposed the polygraph condition at issue here, it specifically noted that the condition is "a tremendous deterrent and satisfies a very legitimate purpose in probationary supervision." J. App. 396. Accordingly, we conclude that the district court did not abuse its discretion in ordering polygraph examinations as part of Boles's sex offender treatment following his most recent conviction.

CONCLUSION

For the reasons set forth above, we **AFFIRM** the judgment in all respects except that we **VACATE** the "risk" condition of supervised release and **REMAND** to the district court for clarification as set forth above.