No. _____

IN THE

Supreme Court of the United States

DANIEL EUGENE COOKSON,
Petitioner,
v.

UNITED STATES OF AMERICA,
Respondent.

On Petition for a Writ of Certiorari to the
United States Court of Appeals for the Tenth Circuit

PETITION FOR A WRIT OF CERTIORARI

MELODY BRANNON
Federal Public Defender
DANIEL T. HANSMEIER
Appellate Chief
Counsel of Record
KANSAS FEDERAL PUBLIC DEFENDER
500 State Avenue, Suite 201
Kansas City, Kansas 66101
Phone: (913) 551-6712
Email: daniel_hansmeier@fd.org
Counsel for Petitioner

QUESTION PRESENTED

This case involves a warrant issued by a federal magistrate judge in the Eastern District of Virginia authorizing the government to install malware on computers associated with a child pornography website (Playpen). The number, identity, and location of these computers was unknown to law enforcement. Thus, the government used this warrant to search computers in locations well beyond Virginia (here, Kansas). Consistent with other lower courts, the Tenth Circuit assumed that this warrant violated the Federal Magistrates Act (28 U.S.C. § 636), Federal Rule of Criminal Procedure 41(b), and the Fourth Amendment. But the Tenth Circuit refused to suppress evidence under the good-faith exception to the exclusionary rule. The question presented is:

> When a warrant authorizes a search beyond the issuing judge's territorial jurisdiction, does the good-faith exception to the exclusionary rule apply to save the illegal and unconstitutional search.

TABLE OF CONTENTS

INDEX TO APPENDIX

TABLE OF AUTHORITIES CITED

Cases

Statutes

Other Authorities

PETITION FOR WRIT OF CERTIORARI

Petitioner Daniel Cookson respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Tenth Circuit.

OPINIONS BELOW

The Tenth Circuit's decision is published at 922 F.3d 1079, and is included as Appendix A. The district court's unpublished order denying Mr. Cookson's motion to suppress is available at 2017 WL 5629678, and is included as Appendix B.

JURISDICTION

This Court has jurisdiction under 28 U.S.C. § 1254(1).

CONSTITUTIONAL AND OTHER PROVISIONS INVOLVED

The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

28 U.S.C. § 636(a)(1) provides:

> (a) Each United States magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law--
>
> > (1) all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts;

Federal Rule of Criminal Procedure 41(b) (2015) provides:

> (b) **Authority to Issue a Warrant**. At the request of a federal law enforcement officer or an attorney for the government:
>
> (1) a magistrate judge with authority in the district -- or if none is reasonably

available, a judge of a state court of record in the district -- has authority to issue a warrant to search for and seize a person or property located within the district;

(2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;

(3) a magistrate judge--in an investigation of domestic terrorism or international terrorism--with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;

(4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and

(5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:

(A) a United States territory, possession, or commonwealth;

(B) the premises--no matter who owns them--of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or

(C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.[1]

[1] Rule 41(b) was amended in 2016 and now includes a subsection (6) that provides:

(6) a magistrate judge with 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 if:

(A) the district where the media or information is located has been concealed through technological means; or
(B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

STATEMENT OF THE CASE

1. This case begins in Virginia. Pet. App. 3a. Around 2014, the FBI learned of a child pornography website – Playpen – that operated on The Onion Router (TOR), a network developed by the U.S. Naval Research Laboratory that is designed to protect online user privacy. Pet. App. 3a. The TOR network can be used for lawful or unlawful purposes. In essence, the use of the network anonymizes the user (i.e., it hides the user's IP address and other identifying information). Pet. App. 3a, 32a.

The FBI tracked down Playpen's operator and arrested him on February 19, 2015. Pet. App. 2a, 33a. But rather than shutter the site, as one might expect law enforcement to do to prevent the dissemination of child pornography, the FBI assumed control of it and operated the site from a government facility in the Eastern District of Virginia for the next two weeks (until March 4, 2015). Pet. App. 3a-4a, 33a; *United States v. Workman*, 863 F.3d 1313, 1315 (10th Cir. 2017). The FBI became a large-scale child-pornography distributor for two weeks for one ostensible reason: "to find the users who were viewing child pornography on Playpen." *Workman*, 863 F.3d at 1315; *see also* Pet. App. 34a ((over 100,000 individuals visited the site during this two-week period). And, of course, these users (all of whom were anonymous thanks to TOR) could have been located anywhere in (or out) of the country. *Workman*, 863 F.3d at 1315.

But the government had a plan: it would install software on its Playpen server that would then install malware on any computer that accessed the Playpen website. Pet. App. 3a-4a; *Workman*, 863 F.3d at 1316. "This malware would search the user's computer for identifying information, such as the Internet Protocol address, and

transmit this information to the FBI." *Workman*, 863 F.3d at 1316. In other words, the government would use malware to search countless computers at unknown locations in order to determine the computers' locations. *Id.*

To do this, the government understood that the Fourth Amendment required it to get a search warrant. *Id.* at 1315. But,

> a paradox existed. The FBI maintained the website in the Eastern District of Virginia, but users were spread out all over the country. Finding those users could prove difficult because of geographic constraints on the FBI's ability to obtain a warrant. *Notwithstanding these constraints*, the FBI obtained a warrant that led to the discovery of hundreds of viewers of child pornography.

Id. (emphasis added); Pet App. 3a-4a. This warrant was signed and authorized by a federal magistrate judge in the Eastern District of Virginia. Pet. App. 4a.

In particular, on February 20, 2015 (the day after the FBI arrested Playpen's operator), FBI special agent Douglas McFarlane applied for the search warrant. Pet. App. 3a. Agent McFarlane averred that he had been an FBI agent since 1996 and had participated in "the execution of numerous warrants involving the search and seizure of computers." App.4 at 320.[2] He acknowledged that "connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state." *Id.* at 327. Agent McFarlane's affidavit provided a wealth of technological knowledge, including various computer-related definitions and a detailed discussion of the TOR network. *Id.* at 323-331.

The affidavit did not request what a typical search warrant requests: to search a specific person, place, or thing for contraband. Instead, the affidavit sought

[2] The warrant affidavit is included in the Appendix filed in the Tenth Circuit.

permission "to use a network investigative technique ("NIT") to investigate the users and administrators of the [Playpen] website." *Id.* at 321. The affidavit averred that this "technique" would be deployed on the Playpen website, which was located in the Eastern District of Virginia. *Id.* at 343. The affidavit described the "technique" as follows: when a user downloads content from the Playpen website, the "technique" "would augment that content with additional computer instructions." *Id.* "When a user's computer successfully downloads those instructions from the [Playpen website], located in the Eastern District of Virginia, the instructions, which comprise the NIT, are designed to cause the user's 'activating' computer to transmit certain information to a computer controlled by or known to the government." *Id.* This information (an IP address and other identifying information) "may assist in identifying the user's computer, its location, and the user of the computer." *Id.* at 344-345; *see also* Pet. App. 3a.

In other words, putting aside the unhelpful phrase "network investigative technique" (which could be almost anything), the warrant sought to install malware on any computer that accessed the Playpen website, regardless of where this computer was located at the time it accessed the website. The malware would essentially identify the otherwise anonymous users of the website and permit law enforcement to learn their locations. "[T]he software would automatically install malware onto the user's computer. This malware would search the user's computer for identifying information." *Workman*, 863 F.3d at 1316.

2. The malware worked, resulting in criminal charges throughout the country. Pet. App. 4a. This case comes from Kansas. It was there that the government infected

Mr. Cookson's computer with malware, caused his computer to send identifying information to the government, and led to his arrest and prosecution in this case. Pet. App. 4a.

Specifically, in June 2017, a federal grand jury in Wichita, Kansas returned a two-count indictment, charging Mr. Cookson in both counts with possession of child pornography, 18 U.S.C. § 2252A(a)(5)(B). Pet. App. 4a. Mr. Cookson moved to suppress the evidence, alleging that the Virginia magistrate judge lacked authority to issue a warrant to search a computer in Kansas. Pet. App. 4a-5a. He relied on the Federal Magistrates Act (28 U.S.C. § 636(a)), Federal Rule of Criminal Procedure 41(b), and the Fourth Amendment. Pet. App. 4a-5a, 36a. The district court agreed that the magistrate judge exceeded her authority in issuing the warrant, but, in light of binding Tenth Circuit precedent (*Workman*), applied the good-faith exception and refused to suppress the evidence. Pet. App. 6a, 37a-38a. Mr. Cookson entered into a conditional plea agreement, reserving his right to appeal the denial of his motion to suppress. Pet. App. 6a.

3. The Tenth Circuit affirmed in light of its prior decision in *Workman*. Pet. App. 17a. Like the district court, the Tenth Circuit held that the good-faith exception saved the unconstitutional search. Pet. App. 11a-12a. The Tenth Circuit disagreed that the good-faith exception should not apply because of facts indicating that the government knew that the federal magistrate judge could not lawfully issue the Playpen warrant. Pet. App. 13a-17a.[3] This timely petition follows.

[3] The government appealed Mr. Cookson's probationary sentence. The Tenth Circuit vacated the sentence and remanded for resentencing. Pet. App. 29a-30a. We do not seek review of that portion of

REASONS FOR GRANTING THE WRIT

This Court should resolve whether the good-faith exception saves a search conducted in a jurisdiction other than the one where the federal magistrate judge had authority to issue the search warrant.

1. At present, the lower courts have uniformly upheld the Playpen search warrant at issue here under the good-faith exception. *United States v. Ganzer*, 922 F.3d 579 (5th Cir. 2019) (collecting cases). But three Circuits – the Second, Eleventh, and D.C. – have yet to decide the issue.

2a. Regardless, the lack of a Circuit split should not dissuade this Court from addressing this extremely important issue. This issue is important in light of the number of defendants affected by the Playpen warrant. *See Workman*, 863 F.3d at 1315 ("the FBI obtained a warrant that led to the discovery of hundreds of viewers of child pornography"); *United States v. Horton*, 863 F.3d 1041, 1045-1046 (8th Cir. 2017) (noting more than 40 such cases). Indeed, given how many people accessed the Playpen website (over 100,000), it is likely that the warrant provided the government with evidence to prosecute thousands of individuals. For that reason alone, this issue is sufficiently important for this Court's review.

b. But review is also necessary because this Court has never addressed the availability of the good-faith exception when the issuing judge lacked authority to issue the warrant in the first place. This unanswered question leaves a void in this Court's good-faith-exception precedent. That precedent holds that the good-faith exception is available where the warrant lacks probable cause, *United States v. Leon*,

---

the Tenth Circuit's decision. Because this petition has nothing to do with Mr. Cookson's sentence, we do not discuss it.

468 U.S. 897, 900 (1984), where the warrant was quashed, *Arizona v. Evans*, 514 U.S 1, 4 (1995), and where the warrant was recalled, *Herring v. United States*, 555 U.S. 135, 138 (2009). But this precedent leaves wholly unanswered the question presented here: whether the good-faith exception saves a search warrant issued by a magistrate judge who had no authority to issue it. This Court should grant certiorari to answer the question.

3. Review is also necessary because the Tenth Circuit's decision is incorrect. At the time the federal magistrate judge issued the Playpen search warrant, Federal Rule of Criminal Procedure 41 only permitted a federal magistrate judge to issue a warrant to search for property located within the magistrate judge's district. Fed.R.Crim.P. 41(b). This rule is consistent with 28 U.S.C. § 636(a), which also limits a federal magistrate judge's jurisdiction (or power) to the district in which the magistrate judge sits. As then-Judge Gorsuch explained, "[s]ection 636(a)'s territorial restrictions are jurisdictional limitations on the power of magistrate judges and the Supreme Court has long taught that the violation of a statutory jurisdictional limitation—quite unlike the violation of a more prosaic rule or statute—is per se harmful." *United States v. Krueger*, 809 F.3d 1109, 1122 (10th Cir. 2015) (Gorsuch, J., concurring). Thus, "a warrant issued for a search or seizure beyond the territorial jurisdiction of a magistrate's powers [is] no warrant at all," and is "invalid under the Fourth Amendment." *Id.* at 1123-1125 (quoting *United States v. Baker*, 894 F.2d 1144 (10th Cir. 1990)).

The good-faith exception exists to protect officers who rely in objective good faith on mistakes made by others. This Court has applied the doctrine in four

circumstances: (1) an officer's good-faith reliance on a subsequently invalidated search warrant, *United States v. Leon*, 468 U.S. 897, 922 (1984); (2) an officer's good-faith reliance on a subsequently invalidated statute, *Illinois v. Krull*, 480 U.S. 340, 359 (1987); (3) an officer's good-faith reliance on a database negligently maintained by others, *Herring v. United States*, 555 U.S. 135, 137 (2009), and *Arizona v. Evans*, 514 U.S. 1 (1995); and (4) an officer's good-faith reliance on binding (but subsequently overruled) appellate precedent, *Davis v. United States*, 564 U.S. 229, 241 (2011).

Only the first exception could possibly apply here, since the officers obtained a warrant to search Mr. Cookson's computer. But the good-faith exception does not inexorably apply whenever officers obtain a warrant. In *Leon*, this Court identified four situations where the good-faith exception would not apply: (1) where the warrant-issuing judge "was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth"; (2) where the warrant-issuing judge "wholly abandon[s] his judicial role"; (3) where the affidavit is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; and (4) where the warrant is "so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Leon*, 468 U.S. at 923.

Here, it's clear that the government in fact misled the warrant-issuing judge into issuing an unauthorized warrant. Rather than ask to install malware on countless computers located in unknown locations, the officers obfuscated the point by asking instead to use a "network investigative technique" on the Playpen website, which

"operates in the Eastern District of Virginia." Pet. App. 3a. At no point did the officers truthfully explain to the magistrate judge the actual logistics of its "network investigative technique."

And there's more. As early as 2009, the Department of Justice's Computer Crime and Intellectual Property Section opined that warrants would violate Rule 41(b) if they authorized searches of computers located outside the district in which the warrant was issued.[4] This publication advised law enforcement to "obtain additional warrants for each location where the data resides to ensure compliance with a strict reading of Rule 41(a). For example, if the data is stored in two different districts, agents should obtain separate warrants from the two districts." *Id.* at 84-85. This publication warned agents that an intentional disregard of Rule 41 would lead to suppression of the evidence. *Id.* at 85-86. This is important here because the lead case agent investigating Playpen – agent Alfin – testified that lawyers with the Computer Crime Section "may have been consulted or involved at some point in time." App.4 at 568.

The Tenth Circuit dismissed this publication because the publication further opines that unlawfully seized evidence "ordinarily should not lead to suppression of the evidence obtained." Pet. App. 14a. But the publication relies on the good-faith exception to draw this conclusion. Pet. App. 14a. And the good-faith exception applies only when a search violates the Fourth Amendment. Thus, the government put itself

[4] *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, DOJ Computer Crime and Intellectual Property Section Criminal Division, at 84, available at: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

on notice that the search conducted here was unconstitutional.

Moreover, there's an exception to this "ordinary" rule (ignored by the Tenth Circuit): "unless the agents intentionally and deliberately disregarded the Rule, or the violation leads to 'prejudice' in the sense that the search might not have occurred." Both apply here. As explained below, the government knew that it could not conduct this search consistent with Rule 41. And there is no question that the search "might not have occurred" had the government not disregarded the rule.

The government also unsuccessfully sought an analogous warrant from a federal magistrate judge in Texas some two years before the government applied for the search warrant at issue here. *In re Warrant*, 958 F.Supp.2d 753 (S.D. Tex. 2013). But the federal magistrate judge denied the application, finding that Rule 41(b) did not authorize it to issue a warrant to install malware on a computer whose location was unknown. *Id.* at 757-758. Thus, when FBI agent McFarlane prepared the warrant affidavit in this case, he was on notice what the plain text of the applicable provisions provided: the federal magistrate judge had no authority to issue the warrant sought.

Additionally, following this decision, the Department of Justice initiated efforts to revise Rule 41 to permit such malware searches. In a September 2013 letter from the acting Assistant Attorney General to the Chair of the Advisory Committee on Criminal Rules, the government sought an amendment to Rule 41 that would permit magistrate judges to issue warrants for electronically stored information "located within or outside that district." Pet. App. 15a. The letter indicated that the proposed amendment "would better enable law enforcement to investigate . . . crimes involving Internet anonymizing technologies." App.4 at 397. It explained the need to "employ

software that enables [law enforcement] through a remote search to determine the true IP address or other identifying information associated with the criminal's computer." *Id.* at 398. In advocating for the rule, the government cited *In re Warrant*. *Id.* This fact is especially important here because agent Alfin testified that higher-up Department of Justice officials and the FBI office of general counsel were involved in the investigation and in obtaining the search warrant. App.4 at 567-570.

The Tenth Circuit found that this letter "lends credence to Mr. Cookson's argument that the FBI was aware of *In re Warrant* and Rule 41(b)'s territorial restrictions." Pet. App. 16a. The Tenth Circuit nonetheless dismissed the letter, claiming that the letter did not show that the government "knew Rule 41(b) in its then-current form did not authorize the [Playpen] warrant." Pet. App. 16a. But the letter candidly admits that Rule 41 "does not directly address the special circumstances" at issue here. Pet. App. 16a. There is no other way to read the letter but as a concession that the government was well aware that the Playpen warrant was not authorized by Rule 41.

And Rule 41 was ultimately amended, after the search at issue here, to authorize "a magistrate judge with authority in any district where activities related to a crime may have occurred" "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" where the location of the information "has been concealed through technological means." Fed.R.Crim.P. 41(b)(6)(A). If the search at issue here were proper (i.e., if the search was authorized by the law as it existed at the time), there would have been no need to amend Rule 41 in this manner.

The Tenth Circuit referred to this amendment as a "clarification" of the rule, but that's simply not true. Pet. App. 17a. Rule 41(b)(6)(A) was *added* to the rule; no part of the rule was "clarified." This new provision did not clarify anything that already existed within the rule; it instead added an entirely new circumstance in which a federal magistrate judge is allowed to issue a search warrant.

This history demonstrates that the government did not act in good faith when it obtained the Playpen warrant. Instead, it knew that the federal magistrate judge had no authority to issue the warrant. The fact that the magistrate judge issued the warrant in any event is not a reason to excuse the search, but is instead a reason to exclude the improperly obtained evidence as obtained in bad faith.

In the end, when a court defies its jurisdiction and acts beyond the lawful bounds of its authority, its order is void (not merely voidable). *Benton v. Maryland*, 395 U.S. 784, 797 (1969). And the distinction between a void order and a voidable order is "not a mere nicety of legal metaphysics." *U.S. Catholic Conference v. Abortion Rights Mobilization, Inc.*, 487 U.S. 72, 77 (1988). It "rests instead on the central principle of a free society that courts have finite bounds of authority, some of constitutional origin, which exist to protect citizens from the very wrong asserted here, the excessive use of judicial power." *Id.* A judge acting without jurisdiction is "not acting as a court"; he is "a pretender to, not a wielder of, judicial power." *United States v. Mine Workers of America*, 330 U.S. 258, 310 (1947) (Frankfurter, J., concurring in the judgment).

Thus, "[a]ll proceedings of a court beyond its jurisdiction are void." *Ex parte Watkins*, 28 U.S. 193, 197 (1830). They have no legal effect whatsoever; it is as if they never happened. The same is true for warrants issued without jurisdiction: they are

"absolutely void." *Young v. Hesse*, 30 F.2d 986, 987 (D.C. Cir. 1929).

Two additional points, First, in *Workman*, the Tenth Circuit relied on *Herring* and *Evans* to excuse the unconstitutional search. This reliance was misplaced. In *Herring* and *Evans*, officers arrested individuals because the officers were told (by a clerk in *Herring*; a computer in *Evans*) that arrest warrants existed for the individuals. *Herring*, 555 U.S. at 137; *Evans*, 514 U.S. at 4. Because the officers did nothing other than rely on the mistake of a third-party, the Supreme Court applied the good-faith exception to the exclusionary rule. *Herring*, 555 U.S. at 147-148; *Evans*, 514 U.S. at 11-16. But here, it was the officers who authored the search warrant affidavit. And as just explained, the officers sought a warrant knowing full well that the federal magistrate judge in Virginia had no authority to issue it. Only if the officers in *Herring* misled the clerk into thinking an arrest warrant existed, or entered the incorrect information into the computer in *Evans*, would those cases be analogous to this one.

Finally, the Tenth Circuit below suggested that the government might have thought the Playpen warrant was authorized as a "tracking device" under Rule 41(b)(4). Pet. App. 17a. But the suggestion that the officers could have thought that Rule 41(b)(4) applied because the malware was a "tracking" device is both factually and legally unsupported. It is factually unsupported because the affidavit did not seek to install a "tracking" device on anything. App.4 at 320-350. It is legally unsupported because the malware was not a "tracking" device, nor would Rule 41(b)(4) apply because the "device" was not attached in Virginia (as the rule requires). App.1 at 130-132. The fact that a very small minority of federal judges bought this no-merit post

hoc theory, Pet. App. 17a, is not a reason to employ the good-faith exception here. The good-faith exception should not apply. Because the Tenth Circuit refused to suppress the evidence, review is necessary.

4. This case is an ideal vehicle to address this issue. Mr. Cookson raised the issue in the lower courts, and the Tenth Circuit decided the issue in a published decision. There are no procedural hurdles to review in this case.

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be granted.

Respectfully submitted,

MELODY BRANNON
Federal Public Defender

DANIEL T. HANSMEIER
Appellate Chief
Counsel of Record
KANSAS FEDERAL PUBLIC DEFENDER
500 State Avenue, Suite 201
Kansas City, Kansas 66101
Phone: (913) 551-6712
Email: daniel_hansmeier@fd.org
Counsel for Petitioner

FILED
United States Court of Appeals
Tenth Circuit

April 26, 2019

Elisabeth A. Shumaker
Clerk of Court

PUBLISH

UNITED STATES COURT OF APPEALS

FOR THE TENTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellant/Cross-Appellee,

v.

DANIEL EUGENE COOKSON,

Defendant-Appellee/Cross-Appellant.

Nos. 18-3070
and 18-3071

Appeal from the United States District Court
for the District of Kansas
(D.C. No. 6:17-CR-10087-JTM-1)

Stephen R. McAllister, United States Attorney (Jason W. Hart, Assistant United States Attorney, with him on the briefs), District of Kansas, Wichita, Kansas, for Plaintiff-Appellant/Cross-Appellee.

Daniel T. Hansmeier, Appellate Chief (Melody Brannon, Federal Public Defender, Timothy J. Henry, Assistant Federal Public Defender, with him on the briefs), Kansas City, Kansas, for Defendant-Appellee/Cross-Appellant.

Before **TYMKOVICH**, Chief Judge, **BACHARACH**, and **McHUGH**, Circuit Judges.

McHUGH, Circuit Judge.

Daniel Eugene Cookson pleaded guilty to two counts of possessing child pornography after the FBI identified him in the course of its large-scale sting operation involving the website "Playpen." At his sentencing hearing, the district court determined Mr. Cookson's criminal history and total offense level correlated to a Guidelines range of 97–121 months. The district court announced its intention to sentence Mr. Cookson to a term of seventy-two months' imprisonment. But after entertaining argument from both parties and inviting Mr. Cookson's allocution, the district court imposed a sentence of five years' probation.

The United States appealed, challenging Mr. Cookson's sentence as substantively unreasonable. Mr. Cookson cross-appealed, arguing the district court erred in refusing to suppress evidence obtained from his computer by the FBI pursuant to a warrant issued in the Eastern District of Virginia

We affirm the district court's suppression ruling based on our decision involving the same warrant in *United States v. Workman*, 863 F.3d 1313 (10th Cir. 2017), but we vacate Mr. Cookson's sentence as unreasonable and remand to the district court for resentencing.

I. BACKGROUND

A. *Search and Seizure*

In 2015, the FBI tracked down and arrested the operator of Playpen, a website that facilitated the distribution of child pornography. Instead of discontinuing Playpen's operations, however, the FBI decided to use the site to locate individuals using it to access child pornography. *Workman*, 863 F.3d at1315.

Finding Playpen's users presented a challenge because Playpen was accessible only through "Tor" (short for "The Onion Router"), a network and software program designed to allow users to browse the internet anonymously. *Id.* at 1315. To access Playpen, users "had to employ [Tor] software that routed . . . connections through [a series of] third-party computers called 'nodes.'" *Id.* By routing connections in this manner, Tor enabled its users to access Playpen without disclosing their IP addresses (unique numbers assigned to a given user's computer, *see United States v. Henderson*, 595 F.3d 1198, 1200 n.1 (10th Cir. 2010)) or other identifying information.

To bypass the steps Playpen took to keep its users anonymous, the FBI, after seizing control of the website, loaded Playpen's contents—pornography and all—onto a government server in the Eastern District of Virginia. *Workman*, 863 F.3d at 1315. The FBI then sought a warrant in the Eastern District of Virginia which would authorize it to deploy a network investigative technique ("NIT") on the government server hosting Playpen. In support of their application for a search warrant, the FBI obtained an affidavit from Agent Douglas Macfarlane explaining the operation of the proposed NIT as follows:

> In the normal course of operation, websites send content to visitors. A user's computer downloads that content and uses it to display web pages on the user's computer. Under the NIT authorized by this warrant, the TARGET WEBSITE [Playpen], which will be located in Newington, Virginia, in the Eastern District of Virginia, would augment that content with additional computer instructions. When a user's computer successfully downloads those instructions from [Playpen] . . . the instructions, which comprise the NIT, are designed to cause the user's . . . computer to transmit certain information [including IP addresses] to a computer controlled by or known to the government. . . . The NIT will not deny the user . . . access to any data or the functionality of the user's computer.

App. at 342–43. Essentially, when someone logged in to Playpen by entering a username and password, the NIT would cause that person's computer to transmit identifying information (including the user's IP address) to the FBI. A magistrate judge in the Eastern District of Virginia signed the warrant, and the FBI operated Playpen with the NIT for approximately two weeks.[1]

On February 22, 2015, someone with the username "shishkabobs" logged into Playpen. Shishkabobs's computer downloaded the NIT, causing it to transmit identifying information to the FBI. Using this identifying information, the government sought an administrative subpoena for the Southern Kansas Telephone Company to identify the physical address associated with the IP address obtained from shiskabobs's computer. Based on information received from the Southern Kansas Telephone Company, the FBI connected shiskabobs's IP address to a home Mr. Cookson shared with his parents and brother in Howard, Kansas. The FBI obtained and executed a search warrant for this home, where they found child pornography on various devices owned by Mr. Cookson. Mr. Cookson later confessed to using Playpen to view child pornography.

The government charged Mr. Cookson with two counts of possessing child pornography under 18 U.S.C. § 2252A(a)(5)(B). Mr. Cookson moved to suppress all evidence derived from the operation of the NIT on his computer, arguing the magistrate

[1] The Playpen NIT resulted in criminal charges throughout the country, meaning many courts, including ours, have reviewed the same NIT warrant for Fourth Amendment violations. *See, e.g.*, *Workman*, 863 F.3d at 1315; *United States v. Levin*, 874 F.3d 316 (1st Cir. 2017); *United States v. Horton*, 863 F.3d 1041 (8th Cir. 2017).

judge in the Eastern District of Virginia lacked authority to issue the NIT warrant and the warrant therefore violated the Fourth Amendment. Specifically, Mr. Cookson argued that magistrate judges generally may not issue warrants for the search of persons or property outside of their district. *See* 28 U.S.C. § 636(a) (provision of the Federal Magistrates Act giving magistrate judges authority "within the district in which [they sit]"). Although he recognized that the version of Fed. R. Crim. P. 41(b) in force at the time created a limited set of exceptions to this general rule, including for warrants concerning the installation of a tracking device, Mr. Cookson contended the exceptions did not include the NIT. He further argued that, if the district court deemed the warrant invalid, the good-faith exception could not save the fruits of the FBI's unconstitutional search from application of the exclusionary rule because (1) the FBI misled the magistrate judge in its warrant application, (2) the magistrate abandoned her judicial role, and (3) the FBI knew the warrant was facially deficient. *See Workman*, 863 F.3d at 1317–18 (setting forth circumstances in which the good-faith exception does not apply).

The district court denied the suppression motion. The court observed that the same NIT warrant in Mr. Cookson's case had been considered by many other trial courts across the country. Most of these courts found the magistrate judge who issued the NIT warrant lacked the authority to do so, yet they declined to suppress evidence obtained as a result of the NIT under the good-faith exception. *See, e.g.*, *United States v. Ammons*, 207 F. Supp. 3d 732 (W.D. Ky. 2016); *United States v. Henderson*, No. 15–CR–00565–WHO–1, 2016 WL 4549108 (N.D. Cal. Sept. 1, 2016); *United States v. Michaud*, No. 3:15–CR–05351–RJB, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016). And while two courts

decided the good-faith exception did not apply and suppressed the evidence, these decisions were later reversed by the courts' respective circuits. *See United States v. Levin*, 874 F.3d 316, 325 (1st Cir. 2017); *United States v. Horton*, 863 F.3d 1041, 1052 (8th Cir. 2017). The Tenth Circuit addressed the NIT warrant in *United States v. Workman*, holding that, even assuming the warrant was invalid, the good-faith exception saved the evidence from suppression. 863 F.3d at 1319–21.

Here, the district court agreed that the Eastern District of Virginia magistrate judge exceeded her authority in issuing the NIT warrant but determined *Workman* governed the outcome of Mr. Cookson's case. Accordingly, the court applied the good-faith exception and denied Mr. Cookson's suppression motion.

B. *Sentencing*

After the district court denied his motion to suppress, Mr. Cookson entered into a plea agreement as to both counts of the indictment. As relevant here, the plea agreement set forth Mr. Cookson's understanding that his plea entailed a maximum sentence of twenty years' imprisonment, various fines and assessments, and a minimum of five years' supervised release. Mr. Cookson and the government also agreed to a conditional plea allowing Mr. Cookson to appeal the district court's suppression decision. The government agreed that Mr. Cookson could remain on bond (under conditions of supervision) pending resolution of his appeal.

Prior to sentencing, Mr. Cookson's probation officer prepared a Presentence Investigation Report ("PSR"). The PSR calculated Mr. Cookson's base offense level as 18. This base offense level increased to 28 due to a number of adjustments pursuant to

U.S.S.G. § 2G2.2, including a two-level increase under U.S.S.G. § 2G2.2(b)(2) because the material involved a prepubescent minor; a four-level increase under U.S.S.G. § 2G2.2(b)(4) because the material involved sadistic or masochistic conduct or other depictions of violence; a two-level increase under U.S.S.G. § 2G2.2(b)(6) because the offense involved the use of a computer, and a five-level increase under U.S.S.G. § 2G2.2(b)(7)(D) because Mr. Cookson possessed more than 600 images of child pornography. The PSR also listed Mr. Cookson's adult criminal convictions, which resulted in a criminal history score of six and placed him in a criminal history category of III.

Based on an offense level of 28 and a criminal history category of III, the PSR calculated a Guidelines range for Mr. Cookson of 97–121 months' imprisonment. Mr. Cookson's convictions entail a maximum term of imprisonment of twenty years, and a minimum term of five years' supervised release.

The parties filed sentencing memoranda. The United States requested a sentence of ninety-seven months' imprisonment followed by five years' supervised release, emphasizing Mr. Cookson's criminal history and the need to avoid unwarranted sentencing disparities between similarly situated defendants. The government stated that the average sentence for offenders within the 97–121 range was seventy months. The government also stated that the 18 U.S.C. § 3553(a) factors supported a within-Guidelines sentence based on Mr. Cookson's (1) use of Tor anonymizing software; (2) continued involvement with child pornography after being caught by his family; (3) involvement in social networks associated with child exploitation; (4) lengthy

involvement with child pornography; (5) sexting with strangers; and (6) involvement with illegal drugs. App. at 171.

Mr. Cookson requested a sentence of five years' probation, focusing on his rehabilitation as shown by holding a job for twenty-one months, being promoted, and recovering from drug addiction. Mr. Cookson also highlighted a policy disagreement with the § 2G2.2 sentencing enhancements, noting they apply in the majority of cases and have been criticized by the U.S. Sentencing Commission and various courts. Mr. Cookson explained that without those enhancements, his Guidelines range would be 24–30 months instead of 97–121.

During the sentencing hearing, the court determined the Guidelines range of 97–121 months had been correctly calculated based on a total offense level of 28 and criminal history category of III. Before hearing from the parties, the court stated the following:

> Having considered these factors and the advisory guidelines, the nature and circumstances of the offense, and Mr. Cookson's history and characteristics, I am of the view that the guidelines range, even the low end of the guideline range, is greater than necessary to serve the purposes of sentencing and it is my intention to sentence Mr. Cookson to a term of confinement of 72 months on each of Counts 1 and 2, those terms to run concurrently and not consecutively; to be followed by five years of supervised release on each of the two counts, those counts to run, again, concurrently and not consecutively.
>
> I believe that sentence is sufficient but not greater than necessary to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offenses, all as set out at 18 U.S.C. Section 3553(a)(2)(A).

App. at 257–58. The court then invited the government to state its position on this tentatively-announced sentence. The government agreed with the sentence of seventy-two

months' imprisonment but reminded the court that Mr. Cookson had used "sophisticated anonymizing technology" (i.e., Tor) and had engaged with an "internet community devoted to child exploitation," which distinguished him from the "mine run" of defendants. App. at 260–62.

The court then heard argument from Mr. Cookson. Defense counsel began by disputing the government's characterization of aggravating factors under § 3553(a), arguing the use of Tor did not indicate a level of technical sophistication because the software is widely available and used for legitimate purposes, and that the government was incorrect in asserting Mr. Cookson had engaged in "production conduct." Defense counsel pointed to letters from Mr. Cookson's family and his employer, as well as the fact Mr. Cookson had overcome a drug addiction, as evidence of "extraordinary rehabilitation." App. at 274. Defense counsel also highlighted the overrepresentation of Mr. Cookson's criminal history—four out of six total points for that history coming from a single misdemeanor marijuana and drug paraphernalia possession charge. Defense counsel noted that Mr. Cookson held a good job, stayed clean, attended counseling, and had made "great strides in his life," to the point where he could continue to "live a drug-free and . . . law abiding lifestyle." App. at 276–77. Defense counsel argued imprisonment would "have [Mr. Cookson] go backwards rather than forwards," and a sentence of probation would allow Mr. Cookson to continue "contributing to society" and personally moving "in a positive direction." App. at 277. Mr. Cookson then allocuted, apologizing for his actions taken "in the midst of drug addiction [and] depression" and stating that he wished to keep his job and "continue working hard on [his] sobriety." Mr.

Cookson asked for a sentence of probation to allow him to "stay on [his] current path of living a healthy, normal life."

After hearing argument from defense counsel and Mr. Cookson's allocution, but before announcing a final sentence, the court stated the following:

> Mr. Cookson, it's pretty obvious that you have made some significant progress in terms of your drug addiction. I have no idea, obviously, where you are in terms of child pornography but I'm not aware of any further activity that came up during the course of the presentence investigation with respect to that.
>
> You do have a good job and the fact that you've been at it for two years speaks volumes. Your family is obviously very supportive and they have seen very positive changes in you over a period of time. It does seem that your criminal history is overrepresented given the fact that four of your six points came out of a misdemeanor marijuana possession charge even with all of the subsequent stuff. And, frankly, these are serious offenses . . . .

App. at 279–280. The court observed that Congress and the Sentencing Commission had "struggled with this area" (presumably, sentencing for child-pornography possession) and they were "hard" and "heartbreaking" cases. And the court recognized that becoming a registered sex offender represented a "very heavy burden." With respect to Mr. Cookson specifically, the court stated:

> I've seen a lot of people through here over the years convicted of these types of offenses. Some are people who literally are social recluses, who are up in their mother's attic or something, that's where they spend their time, they have no social life at all, any employment that they have they just go to work and they go home and there's no life even there, and you seem to be the exception to the norm. And I intend to give you credit for the fact that you did go out, you did get a job, [and] the fact that you're doing well with it . . . .

App. at 282.

The court then sentenced Mr. Cookson to five years' probation, noting it "would have been more inclined not to place [Mr. Cookson] on probation," but it was concerned

about imprisoning Mr. Cookson while his appeal was pending because his convictions could be overturned. App. at 283. The government objected to the sentence on procedural and substantive grounds, specifically noting its "procedural objection" to the court's apparent reliance on a concern about imprisoning Mr. Cookson pending resolution of his appeal, because the government had agreed Mr. Cookson could remain on bond for that period.

The court later produced a written "statement of reasons" for its sentence, checking boxes for the following reasons for a variance under 18 U.S.C. § 3553(a): "the history and characteristics of the defendant" (including the fact that his criminal history had been "over-represented"); "to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;" "to afford adequate deterrence to criminal conduct;" "to protect the public from further crimes of the defendant;" "to provide the defendant with needed educational or vocational training;" "to provide the defendant with other correctional treatment in the most effective manner;" and based on the district court's "policy disagreement with the guidelines," specifically § 2G2.2.

II. DISCUSSION

A. *NIT Search*

At the outset, the parties do not dispute whether the NIT constituted a search within the meaning of the Fourth Amendment, whether the warrant was valid, or whether the search was reasonable despite the invalid warrant. The only issue before us is whether

the good-faith exception to the exclusionary rule applies to the government's search using the NIT. We decided it did in *Workman*.

There, we assumed the NIT search "violate[d] the Federal Magistrates Act [§ 636(a)] and the Federal Rules of Criminal Procedure." *Workman*, 863 F.3d at 1321. But we explained that under *United States v. Leon*, 468 U.S. 897 (1984), even "improperly obtained evidence remains admissible when the executing agents 'act with an objectively reasonable good-faith belief that their conduct is lawful or when their conduct involves only simple, isolated negligence.'" *Id.* at 1317 (quoting *Davis v. United States*, 564 U.S. 229, 238 (2011)) (internal quotation marks omitted). Because we "expect agents executing warrants to be reasonably well-trained, but we do not expect them to understand legal nuances the way that an attorney would," we concluded in *Workman* that FBI agents could have reasonably relied on the warrant issued by the magistrate in the Eastern District of Virginia when executing the NIT search. *Id.* at 1320–21 (internal quotation marks omitted). Had the agents possessed "sophisticated legal training, they might have recognized" the problems posed by Rule 41(b) and 28 U.S.C. § 636(a), but we do not hold law enforcement to such a standard. *Id.* at 1320. We also observed that eight federal judges had held the NIT warrant complied with federal law and federal rules, suggesting the agents could reasonably "have made the same mistake" when acting in reliance on the warrant. *Id.* at 1321 (noting "objective reasonableness sometimes turns on the clarity of existing law"); *see United State v. Gonzales*, 399 F.3d 1225, 1228–29 (10th Cir. 2005) ("[O]fficers are generally not required to second-guess the magistrate's decision in granting a warrant.").

Although Mr. Cookson recognizes *Workman* involved the same warrant at issue in this case, he argues the record before us contains four new facts that alter the good-faith calculus under *Leon*. We evaluate each of these four facts not expressly considered by *Workman* in turn.

First, Mr. Cookson points to an internal guidance document produced by the Department of Justice—Computer Crime & Intellectual Prop. Section, Criminal Div., U.S. Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (3d ed. 2009), http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf. This manual advised law enforcement to ensure compliance with Fed. R. Crim. P. 41 by "obtain[ing] multiple warrants if they have reason to believe that a network search will retrieve data stored in multiple locations." *Id.* at 84. Mr. Cookson argues the manual advises law enforcement to "obtain additional warrants for each location where the data resides" to ensure compliance with Rule 41(b), 2nd Br. on Cross-Appeal at 26, and therefore it suggests that FBI agents (who "worked very closely with the Department of Justice" during the NIT operation, App. at 568) knew the NIT warrant would violate Rule 41(b). A fuller reading of the manual, however, reveals the DOJ bifurcated its advice depending on whether agents would be able to learn, prior to searching, whether the data searched was located within or without the district. Computer Crime & Intellectual Prop. Section, *supra*, at 84 ("Agents may in some cases be able to learn where the data is located before the search, but in others they will be unable to know the storage site of the data until after the search is completed."). When "agents can learn prior to the search that some or all of

the data described by the warrant is stored in a different location than where the agents will execute the search," the manual advises agents to obtain multiple warrants. *Id.* at 84–85. "When agents do not and even cannot know that data searched from one district is actually located outside the district," the manual expressly advises agents that "evidence seized remotely from another district *ordinarily should not lead to suppression of the evidence obtained*." *Id.* at 85 (emphasis added). The manual goes on to explain that courts will likely *not suppress* the evidence as either (1) obtained in compliance with Rule 41; or (2) even if in violation of Rule 41, obtained in a good-faith manner. *See id.* at 85 (citing *United States v. Ramirez*, 112 F.3d 849, 852 (7th Cir. 1997); *United States v. Denman*, 100 F.3d 399, 402 (5th Cir. 1996); *United States v. Rodriguez*, 968 F.2d 130, 135–36 (2d Cir. 1992)). Because the Tor software used to access Playpen concealed users' IP addresses, agents could not know that data searched pursuant to the NIT warrant was located outside the Eastern District of Virginia. Accordingly, the manual, far from suggesting agents acted in bad faith when obtaining or relying on the NIT warrant, gives support for the FBI's conclusion that the warrant met constitutional muster.

Second, Mr. Cookson points to *In re Warrant*, 958 F. Supp. 2d 753 (S.D. Tex. 2013), in which a magistrate judge denied the FBI's request for a warrant authorizing it to "surreptitiously install data extraction software" on a computer whose location was unknown. *Id.* at 755. Once installed, the software would search the computer for information, activate the computer's built-in camera, and transmit extracted data back to the FBI within the Southern District of Texas. *Id.* The magistrate judge held the warrant application satisfied none of the Rule 41(b) criteria. *Id.* at 756.

The facts of *In re Warrant* bear substantial similarity to those before us. Nevertheless, *In re Warrant* is insufficient to show the FBI lacked good faith when relying on the NIT warrant because magistrate judges differed on the question at the time. *In re Warrant* itself mentions that "in 2007 a magistrate judge is known to have issued a warrant authorizing a similar investigative technique to track the source of e-mailed bomb threats against a Washington state high school." *Id.* at 756 n.2. Likewise, a separate NIT warrant appears to have been issued against a Tor-based child pornography website in 2012. *See United States v. Laurita*, No. 8:13CR107, 2016 WL 4179365, at *3 (D. Neb. Aug. 5, 2016) ("Pursuant to court authorization, a NIT was installed on Website A during the period of November 16, 2012, and December 2, 2012."). This disagreement among magistrate judges supports *Workman*'s conclusion that the FBI reasonably deferred to the issuing magistrate's judgment on a question of unsettled law. *See* 863 F.3d at 1321 ("[O]bjective reasonableness sometimes turns on the clarity of existing law.").

Third, Mr. Cookson points to a September 2013 letter from the acting Assistant Attorney General ("AAG") to the Chair of the Advisory Committee on Criminal Rules. Letter from Mythili Raman, Acting Attorney Gen., to Judge Reena Raggi, Chair, Advisory Committee on the Criminal Rules (Sept. 18, 2013). In this letter, the AAG proposes an amendment to Rule 41 that would allow a magistrate judge "in a district where activities related to a crime have occurred to issue a warrant—to be executed via remote access—for electronic storage media and electronically stored information located within or outside that district." App. at 397. This letter cites *In re Warrant*, observing:

> [E]ven when investigators can satisfy the Fourth Amendment's threshold for obtaining a warrant for [a] remote search . . . a magistrate judge may decline to issue the requested warrant. For example, in a fraud investigation, one magistrate judge recently ruled that an application for a warrant for a remote search did not satisfy the territorial jurisdiction requirements of Rule 41.

Id. at 398. Although this letter lends credence to Mr. Cookson's argument that the FBI was aware of *In re Warrant* and Rule 41(b)'s territorial restrictions, it does not suggest the AAG believed the magistrate judge's decision in *In re Warrant* was correct. Rather, the AAG sought an amendment to Rule 41(b) because the rule "does not directly address the special circumstances that arise when officers execute search warrants, via remote access, over modern communications networks such as the Internet." App. at 397. The AAG hoped to "clarify" the rule because "while the Fourth Amendment permits warrants to issue for remote access to electronic storage media or electronically stored information, Rule 41's language does not anticipate those types of warrants in all cases." *Id.* at 399. Accordingly, the AAG letter does not show the AAG (or, by extension, the FBI) *knew* Rule 41(b) in its then-current form did not authorize the NIT warrant.

Finally, Mr. Cookson notes that Rule 41 was amended in 2016 to allow a magistrate judge to "issue a warrant to use remote access to search electronic storage media . . . within or outside [her] district if . . . the district where the media or information is located has been concealed through technological means." Fed. R. Crim. P. 41(b)(6)(A). The parties do not dispute that this amendment, had it been adopted two years earlier, would have expressly authorized the NIT warrant. But we disagree with Mr. Cookson's contention that "there would have been no need to amend Rule 41" had the NIT search been authorized at the time. 2nd Br. on Cross-Appeal at 28. The amendment

fails to show the FBI's lack of good faith for the same reason the AAG letter does—the amendment of Rule 41 is consistent with an aim to *clarify*, but not necessarily *change*, the rule. Therefore, the proposed and actual amendment bear no clear indications that the pre-amendment Rule 41 forbade the NIT warrant, let alone that the FBI knew as much.

Taken together, Mr. Cookson's four new facts, at most, support *Workman*'s conclusion that the territorial restrictions of Rule 41(b) were unclear at the time the NIT warrant issued. *See* 863 F.3d at 1321. A review of decisions before and since confirms courts could and did differ on, for example, whether the NIT amounted to a "tracking device" expressly authorized by Rule 41. *Compare, e.g.*, *United States v. Jones*, 230 F. Supp. 3d 819, 824–25 (S.D. Ohio 2017), *with Ryan Anthony Adams*, 2016 WL 4212079, at *6 ("[T]he NIT does not track; it searches."). Accordingly, these new facts do not remove us from *Workman*'s ambit, and we decline Mr. Cookson's invitation to distinguish or overrule binding precedent.

B. *Sentencing*

On appeal, the government challenges Mr. Cookson's five-year probationary sentence as substantively unreasonable and purports to waive any challenge as to the sentence's procedural reasonableness. Yet much of the government's argument focuses on the district court's explanation for Mr. Cookson's sentence—specifically its brevity, reliance on a misunderstanding of the terms of Mr. Cookson's plea agreement, failure to consider various § 3553(a) factors, and unexplained deviation from an initially-announced seventy-two-month period of imprisonment. We typically consider such arguments as pertaining to a sentence's procedural reasonableness. *United States v.*

Huckins, 529 F.3d 1312, 1317 (10th Cir. 2008) ("Procedural reasonableness addresses whether the district court incorrectly calculated . . . the Guidelines sentence, treated the Guidelines as mandatory, failed to consider the § 3553(a) factors, relied on clearly erroneous facts, or failed to adequately explain the sentence.") Indeed, the government itself framed some of these objections as "procedural" at Mr. Cookson's sentencing hearing.

Still, we have recently acknowledged a blurring of the line between procedural and substantive reasonableness when it comes to the district court's explanation for a given sentence. *See United States v. Barnes*, 890 F.3d 910, 917 (10th Cir. 2018). Therefore, after stating the standard for our review of the district court's sentencing decision, we review the distinction between procedural and substantive reasonableness and its impact on our decision before evaluating the substantive reasonableness of Mr. Cookson's sentence.

1. Standard of Review

We review a district court's sentencing decision for substantive reasonableness under an abuse-of-discretion standard, looking at the "totality of the circumstances." *United States v. Balbin-Mesa*, 643 F.3d 783, 787 (10th Cir. 2011). "A district court abuses its discretion when it renders a judgment that is arbitrary, capricious, whimsical, or manifestly unreasonable." *United States v. Friedman*, 554 F.3d 1301, 1307 (10th Cir. 2009). Our abuse-of-discretion standard applies "without regard to whether the district court imposes a sentence within or outside the advisory guidelines range," so we do not apply a presumption of unreasonableness to sentences outside the guidelines range. *Id.*

Instead, we "give due deference to the district court's decision that the § 3553(a) factors, on [the] whole, justify the extent of the variance." *Id.* (quotation marks omitted). "That we might reasonably have concluded a different sentence was appropriate is insufficient to justify reversal of the district court." *Id.* (quotation marks and alterations omitted). We bear in mind that the "sentencing judge is in a superior position to find facts and judge their import under § 3553(a) in the individual case," *Gall v. United States*, 552 U.S. 38, 51 (2007), because "[t]he judge sees and hears the evidence, makes credibility determinations, has full knowledge of the facts and gains insights not conveyed by the record." *United States v. Barnes*, 890 F.3d 910, 915–16 (10th Cir. 2018) (quoting *Gall*, 552 U.S. at 51). Finally, "when we review a downward variance from the recommended guidelines range, as we do here, even more solicitude to the sentencing court is appropriate." *Id*. at 916.

2. Procedural Versus Substantive Unreasonableness

In the wake of *United States v. Booker*, 543 U.S. 220 (2005), which converted the mandatory federal sentencing scheme into a discretionary one, we review sentences imposed by the district court for reasonableness. *Friedman*, 554 F.3d at 1307. Our reasonableness review has two aspects: procedural and substantive. *Id.* When reviewing a sentence for procedural reasonableness, we consider "whether the district court committed any error in calculating or explaining the sentence." *Id.*; *see also Gall*, 552 U.S. at 51 (stating appellate courts must first "ensure that the district court committed no significant procedural error, such as failing to calculate (or improperly calculating) the Guidelines range, treating the Guidelines as mandatory, failing to consider the § 3553(a)

factors, selecting a sentence based on clearly erroneous facts, or failing to adequately explain the chosen sentence . . . ."). When reviewing a sentence for substantive reasonableness, we focus on "whether the length of the sentence is reasonable given all the circumstances of the case in light of the factors set forth in 18 U.S.C. § 3553(a)." *Friedman*, 554 F.3d at 1307 (quotation marks omitted).

This distinction turns murky, however, when we consider that the district court's explanation for a given sentence serves a "dual purpose." *See Barnes*, 890 F.3d at 917. First, a district court's explanation of how the § 3553(a) factors apply "is a procedural requirement," *id.*, and the "absence of explanation could constitute procedural error" as could the failure to address a defendant's material, non-frivolous arguments under the § 3553(a) factors. *United States v. Lente*, 647 F.3d 1021, 1031, 1035 (10th Cir. 2011). Second, the content of the district court's explanation "is relevant to whether the length of the sentence is substantively reasonable" because "[a] sentence is more likely to be within the bounds of reasonable choice when the court has provided a cogent and reasonable explanation for it." *Barnes*, 980 F.3d at 917. Stated another way, we rely on the district court's procedurally-required explanation in order to conduct "meaningful appellate review" of a sentence's substantive reasonableness. *Gall*, 552 U.S. at 50; *see Lente*, 647 F.3d at 1039 (explaining that "[w]e cannot fulfill our appellate role, however deferential, in assessing the substantive reasonableness of [a] sentence" without an adequate explanation from the district court). A limited, brief, or inconsistent explanation hinders our ability to do so, and therefore "put[s] at risk the substantive reasonableness of any decision [the district court] reached." *United States v. Lychock*, 578 F.3d 214, 220

(3d Cir. 2009) (quoting *United States v. Goff*, 501 F.3d 250, 256 (3d Cir. 2007)); *see Friedman*, 554 F.3d at 1312 ("[T]he very limited nature of the record and the paucity of reasoning on the part of the district court most certainly bear on our review of the substantive reasonableness of Friedman's sentence."); *United States v. Gonzalez*, 529 F.3d 94, 98 (2d Cir. 2008) ("Determination of whether the sentence is unreasonable is hampered by the brevity of the reasons given for it."). This is especially true when the sentence varies greatly from the sentencing Guidelines, because "a major [variance] should be supported by a more significant justification than a minor one." *Gall*, 552 U.S. at 50.

But the heavier our reliance on the inadequacy of the district court's explanation in holding Mr. Cookson's sentence substantively unreasonable, the less our decision restricts the "bounds of reasonable choice" available to the district court in crafting a sentence on remand. *Barnes*, 890 F.3d at 917. A sentence deemed substantively unreasonable primarily because of an explanation too brief or cursory to justify the extent of its variance from the Guidelines might be substantively reasonable given a more detailed explanation. *See United States v. Park*, 758 F.3d 193, 202 (2d Cir. 2014) ("In holding that the District Court's probationary sentence was *substantively unreasonable*, we rely heavily upon the District Court's own evaluation of the case, as revealed by its statements at the sentencing hearing. . . . We thus do not foreclose the possibility that the imposition of a probationary sentence on remand, after appropriate consideration of the § 3553(a) factors thus far left unaddressed, could be *substantively reasonable* as well.").

With that backdrop in place, we consider Mr. Cookson's sentence in light of "all the circumstances of the case," *Friedman*, 554 F.3d at 1307, using the district court's explanation for the sentence "to assist us in determining whether the district court abused its discretion in weighing the § 3553(a) factors," *Barnes*, 890 F.3d at 917.

3. Substantive Reasonableness Review

18 U.S.C. § 3553(a) requires district courts to consider seven factors in sentencing: (1) the nature and circumstances of the offense and the history and characteristics of the defendant; (2) the need for a sentence to reflect the "basic aims of sentencing, namely (a) 'just punishment' (retribution), (b) deterrence, (c) incapacitation, and (d) rehabilitation," *United States v. Walker ("Walker I")*, 844 F.3d 1253, 1253 (10th Cir. 2017); (3) the kinds of sentences available; (4) the Sentencing Commission Guidelines; (5) Sentencing Commission policy statements; (6) the need to avoid unwarranted sentencing disparities; and (7) the need for restitution. *See* 18 U.S.C. § 3553(a)(1)–(7).

The district court explained Mr. Cookson's sentence primarily in terms of § 3553(a)(1), specifically referencing Mr. Cookson's (1) recovery from drug addiction, (2) success in a new job, and (3) support from his family. The court acknowledged that Mr. Cookson's offenses were serious and that possession of child pornography causes significant harm to the children depicted. *See United States v. DeRusse*, 859 F.3d 1232, 1239 (10th Cir. 2017) ("Viewing the entire sentencing transcript in context . . . we are convinced that the district court was fully aware of the seriousness of the offense and took very seriously the harm suffered by the [victims].") But after hearing argument from

defense counsel about Mr. Cookson's three-year recovery from addiction and from Mr. Cookson himself attributing his conduct to "a bad place in [his] life at the time in the midst of drug addiction [and] depression," App. at 278, the district court remarked that Mr. Cookson's pre-sentencing rehabilitation made him the "exception to the norm," App. at 282. The district court observed that Mr. Cookson had obviously made "significant progress in terms of . . . drug addiction," App. at 279, and that Mr. Cookson had "a good job and the fact that [Mr. Cookson has] been at it for two years speaks volumes," *id.* at 280. Finally, the court noted, "It does seem that [Mr. Cookson's] criminal history is overrepresented given the fact that four of [his] six points came out of a misdemeanor marijuana possession charge."[2] App. at 280. The combination of these circumstances could reasonably support a downward variance, even a large one, under 18 U.S.C. § 3553(a)(1). *See Walker I*, 844 F.3d at 1257.

The district court's written statement of reasons also expressed its policy disagreement with U.S.S.G. § 2G2.2 as a reason for the downward variance. We have described arguments criticizing the § 2G2.2 enhancements as "quite forceful" and have "specifically cautioned district courts to carefully apply the child pornography distribution guideline and remain mindful that they possess broad discretion in fashioning sentences under § 2G2.2." *United States v. Wireman*, 849 F.3d 956, 962 (10th Cir. 2017) (internal quotation marks and alterations omitted); *see also United States v. Grigsby*, 749

[2] The court's written statement of reasons makes clear that it weighed this fact under § 3553(a)(1), although an over-represented criminal history could also support a downward departure under U.S.S.G. § 4A1.3(b)(1).)

F.3d 908, 911 (10th Cir. 2014) (referencing a "number of reported cases where district courts have rejected application of § 2G2.2 for want of an empirical basis"); *United States v. Dorvee*, 616 F.3d 174, 186–87 (2d Cir. 2010) (noting that the ubiquitous application of the § 2G2.2 enhancements resulted in "virtually no distinction between the sentences for defendants [who merely possessed child pornography] . . . and the sentences for the most dangerous offenders who, for example, distribute child pornography for pecuniary gain"). Accordingly, the district court did not abuse its discretion in determining that its policy disagreement with § 2G2.2 could support the imposition of a more lenient sentence. But the court did not elaborate on this policy disagreement during the sentencing hearing except to say that "Congress has struggled with this area" and "the Sentencing Commission has struggled with this area." App. at 280. Nor did the court address the extent to which the disagreement weighed in its final decision. Instead, the court's explanation focuses overwhelmingly on Mr. Cookson's presentencing rehabilitation and its desire not to see Mr. Cookson's progress "turned back." *Id.* at 283.

Although we recognize these concerns as valid, we have cautioned against excessive reliance on a single factor in sentencing. In *Walker I*, we held substantively unreasonable a time-served sentence for a serial bank robber who pleaded guilty to two bank robberies. *See* 844 F.3d 1255.[3] We reasoned the district court had focused "almost

[3] On remand, the district court resentenced Mr. Walker to ten years of probation, two years of home confinement, and 500 hours of community service. *United States v. Walker (Walker II)*, 918 F.3d 1134, 1137 (10th Cir. 2019). The government appealed again, arguing that the district court violated *Walker I*'s mandate by declining to sentence

exclusively on Mr. Walker's newfound sobriety" and had paid "inadequate attention" to a number of other statutory factors, including the "basic aims of punishment" and the need to avoid unwarranted sentencing disparities, in deciding to impose a time-served sentence. *Id.* 1258–59; *see* 18 U.S.C. § 3553(a)(1), (6). Although the district court in *Walker I* discussed, for example, the values of specific deterrence and rehabilitation, we criticized its failure to mention incapacitation and its offhand "dismiss[al] [of] the relevance of [general] deterrence." *See Walker I*, 844 F.3d at 1257–58. Of course, the district court need not afford equal weight to each § 3553(a) factor, *United States v. Sanchez-Leon*, 764 F.3d 1248, 1267 (10th Cir. 2014), and we will defer on substantive-reasonableness review "not only to a district court's factual findings but also to its determinations of the weight to be afforded to such findings." *United States v. Smart*, 518 F.3d 800, 808 (10th Cir. 2008). Unlike the district court in *Walker I*, however, the court here made no mention of deterrence, rehabilitation, or incapacitation in explaining Mr. Cookson's sentence. Nor did it address the potential for "unwarranted sentencing disparities" raised by the government. Although we can extrapolate reasoning from the district court's relatively brief explanation—for example, the district court might have viewed any disparity resulting from Mr. Cookson's sentence as a "warranted" one, *see Lente*, 759 F.3d at 1169 (explaining that "[o]ur sentencing scheme seeks to eliminate not

---

Mr. Walker to a prison term. *Id.* at 1143. We disagreed because *Walker I*'s mandate "did not specifically limit the district court's discretion by requiring it to impose a sentence of imprisonment." *Id.* at 1154. We declined to express any view on whether the new sentence was substantively reasonable, "as the government waived its argument on that point by failing to adequately address the district court's analysis." *Id.*

all sentencing disparities, but only unwarranted disparities") (internal quotation marks omitted)—the explanation itself does little to assist us in understanding how it applied the § 3553(a) factors other than § 3553(a)(1) to Mr. Cookson's case, *see Barnes*, 890 F.3d at 917. Without any explanation from the district court on the weight it afforded the other § 3553(a) factors in granting Mr. Cookson such a large variance, we consider the sentence as substantively unreasonable. *See Smart*, 518 F.3d at 808; *see also Gall*, 552 U.S. at 50 ("[A] major [variance] should be supported by a more significant justification than a minor one.").

Comparing the district court's explanation of Mr. Cookson's sentence with other recent cases upholding the substantive reasonableness of large downward variances supports this conclusion. *Barnes*, for example, considered a large downward variance for former jail employees convicted of conspiracy to violate, and deprivation of, constitutional rights related to abuse they inflicted on the jail's inmates. *See* 890 F.3d at 914 (affirming a downward variance from a Guidelines range of 70–87 months' imprisonment to a twenty-four-month sentence followed by twenty-four months' supervised release for the first defendant and a twelve-month sentence followed by thirty-six months' supervised release for the second). In upholding the sentences as substantively reasonable, we credited the district court with a "careful" discussion, in which the court "walked through" and "properly addressed each of the § 3553(a) factors before approving a downward variance from the Guidelines range." *Id.* at 918. The *Barnes* district court expressly considered, for example, the defendants' personal characteristics, their risk of recidivism, the "specific and general deterrence" advanced by

their sentences, and the seriousness of their offenses. *Id.* at 918–19. Likewise, in *DeRusse*, we affirmed a downward departure and variance from a Guidelines range of 108–135 months to a sentence of time served followed by five years' supervised release in a kidnapping case. 859 F.3d at 1235–36. We distinguished the district court's explanation of DeRusse's sentence from that in *Walker I*, describing it as having "thoughtfully considered all of the § 3553 factors, rather than focusing almost exclusively on one particular factor, and concluded based on its assessment of all of these factors that a sentence of time-served would be the most appropriate." *Id.* at 1240.

Here, the district court's assessment, in addition to focusing almost exclusively on § 3553(a)(1), relied on an apparent misunderstanding of Mr. Cookson's conditional plea agreement. Fearing that Mr. Cookson's challenge to the suppression ruling might be successful, and that Mr. Cookson would then have spent time in prison and lost his job only for the charges against him to be dismissed, the court stated it would have been less inclined to place Mr. Cookson on probation but for his conditional plea. But the government had consented in the conditional plea agreement that Mr. Cookson could remain on bond pending resolution of his appeal. The district court's concern was thus unfounded, and its suggestion that it would have been more inclined to sentence Mr. Cookson to a term of imprisonment absent this concern gives us pause in deferring to its "decision that the § 3553(a) factors, on [the] whole, justify the extent of the variance." *Friedman*, 554 F.3d at 1307.

In light of this discrepancy, and because the district court placed nearly exclusive focus on Mr. Cookson's presentencing rehabilitation in explaining its decision, the

sentence it imposed is substantively unreasonable. We reach this conclusion, in large part, based on the significant variance in Mr. Cookson's sentence and the district court's limited and inconsistent explanation for that variance. *See Barnes*, 890 F.3d at 917 ("A sentence is more likely to be within the bounds of reasonable choice when the court has provided a cogent and reasonable explanation for it."). We therefore decline the government's request that we direct the district court to impose the seventy-two-month sentence it tentatively announced at the outset of Mr. Cookson's sentencing hearing. *See Koon v. United States*, 518 U.S. 81, 97 (1996) ("[I]t is not the role of an appellate court to substitute its judgment for that of the sentencing court as to the appropriateness of a particular sentence.") (quoting *Williams v. United States*, 503 U.S. 193, 205 (1992)). Nor do we agree the district court's deviation from its tentatively-announced seventy-two-month sentence should weigh heavily in our assessment of whether it reached a substantively unreasonable decision.[4] To the contrary, the record indicates the district

[4] The government cites a single case, *United States v. Gerezano-Rosales*, 692 F.3d 393 (5th Cir. 2012), in support of its argument that the district court's tentatively-announced sentence should affect our reasonableness determination. But what the government characterizes as an "initial announcement" of a sentence in *Gerezano-Rosales*, 3rd Br. on Cross-Appeal at 9, was in fact the final sentence imposed by the district court after giving the defendant the opportunity to allocute. *Gerezano-Rosales*, 692 F.3d at 396. Immediately after sentencing the defendant to seventy-one months, the district court attempted to impose a 108-month sentence because the defendant had been "disrespectful when he questioned the appropriateness of the originally imposed" sentence. *Id.* at 400. The appellate court invalidated the higher sentence as substantively unreasonable because "no matter how insolently Gerezano delivered his retorts to the district court, his statements could not have reasonably justified a variance of three years above the guidelines range, especially since the court had previously found that a Guidelines sentence was otherwise appropriate." *Id.* at 402. This case bears little resemblance to Mr. Cookson's, in which the district court announced its inclination to impose a seventy-two-month sentence as a starting point for discussion. *See United States*

court, after announcing a tentative sentence, listened carefully to counsel's arguments and Mr. Cookson's allocution.[5] Something about these arguments apparently persuaded the district court to change its mind and impose a more lenient sentence than it had initially anticipated. *See* App. at 283 (explaining the district court "came in . . . not expecting to [impose a probationary sentence]"). But the district court undertook a relatively brief explanation of the statutory factors supporting the sentence it finally imposed, which impedes our review. We therefore do not foreclose the possibility that a more detailed explanation from the district court of the weight it afforded § 3553(a) factors other than § 3553(a)(1) could yield a similar, but substantively reasonable, sentence on remand. *See Park*, 758 F.3d at 202.

III. CONCLUSION

For these reasons, we **AFFIRM** the district court's denial of Mr. Cookson's motion to suppress the fruits of the NIT search of his computer. We also **VACATE** the

v. Valdez-Aguirre, 861 F.3d 1164, 1165 (10th Cir. 2017) (explaining "[f]ederal trial courts frequently approach sentencing with at least some idea of what they intend to impose," and therefore "sometimes announce a sentence before giving the defendant an opportunity to allocute").

[5] Fed. R. Crim. P. 32(i)(4)(A)(ii) requires as much. Had the district court refused to listen to Mr. Cookson's allocution and stubbornly held to its tentative sentence, it may have violated Mr. Cookson's right to allocute. *United States v. Theis*, 853 F.3d 1178, 1182 (10th Cir. 2017) ("A court violates this right to allocute when it definitively announces the defendant's sentence before giving him an opportunity to speak, and fails to communicate to the defendant that it will genuinely reconsider the sentence in light of his remarks.").

district court's decision sentencing Mr. Cookson to five years' probation and **REMAND** for resentencing.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

UNITED STATES OF AMERICA,

Plaintiff,

v. Case No. 17-10087-1-JTM

DANIEL EUGENE COOKSON,

Defendant.

MEMORANDUM AND ORDER

The instant prosecution is the result of an FBI investigation into Playpen, a website that facilitated the distribution of child pornography. Through a series of events, the FBI learned that defendant accessed Playpen from his home, and the government charged defendant with two counts of possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). Presently before the court is defendant's motion to dismiss (Dkt. 14) alleging that the government committed outrageous conduct. Defendant also moves to suppress all evidence derived from the search of his home computer, subsequent search of his residence, and statements made to the FBI (Dkt. 13). Defendant further moves for discovery (Dkt. 15). For the reasons stated below, defendant's motions to dismiss and suppress evidence are denied. Defendant's motion for discovery is denied without prejudice.

I. Background[1]

Playpen operated on the "The Onion Router" or "Tor" network, which provides more anonymity to its users than the regular Internet. The Tor was developed by the U.S. Naval Research Laboratory and is now accessible to the general public. Tor users must download special software that lets them access the network. When a user accesses the Tor, communications from that user are routed through a system of network computers that are run by volunteers around the world. When a user connects to a website, the only Internet Protocol ("IP") address that the website "sees" is the IP address of the last computer through which the user's communications were routed. This final relay is called an exit node. Because there is no practical way to trace a user's communications from the exit node back to the user's computer, Tor users are effectively anonymous to the websites they visit.

The Tor also provides anonymity to the individuals who run websites or forums on it. Websites may be set up on the Tor as "hidden services" that are only accessed through the Tor. The IP address is replaced with a Tor-based address, which consists of a series of alphanumeric characters followed by ".onion." There is no way to look up the IP address of the computer hosting a hidden service.

Tor users cannot simply perform a search to find a hidden service that may interest the user. Instead, a user must know the Tor-based address of the hidden service. As a result, a user cannot simply stumble onto a hidden service. The user may

[1] The majority of this background information is taken from the warrant application and supporting affidavit attached to defendant's motion to suppress (Dkt. 13-1).

obtain the address from postings on the Internet or by communications with other Tor users. One hidden service may also link to another.

Playpen was a hidden service contained on the Tor, and it had been linked to by another hidden service that was dedicated to child pornography. In December 2014, a foreign law enforcement agency informed the FBI that it suspected a United States-based IP address belonged to Playpen. In January 2015, after obtaining a search warrant, the FBI seized the IP address and copied the contents of the website. On February 19, 2015, the FBI arrested the individual suspected of administering Playpen.

The FBI seized control of Playpen, however, it could not easily identify Playpen users. Thus, the FBI obtained a warrant from an E.D. Va. magistrate judge allowing them to use a network investigative technique ("NIT") to locate the administrators and users of Playpen—including installing software onto the FBI's Playpen server in Virginia. The NIT installed itself as soon as a user logged into Playpen and reached the landing page; installation did not require any confirmed downloads of child pornography. Once installed, the NIT would search the user's computer for identifying information, such as the IP address, and transmit this information back to the FBI via the Playpen server located in the E.D. Va.

The FBI operated Playpen with the NIT from approximately February 20, 2015, to March 4, 2015. On February 22, 2015, a visitor named "shishkabobs" logged into Playpen, and the NIT was installed on shishkabobs's computer.

On March 26, 2015, the FBI used some of the data it had collected from shishkabobs's computer to obtain an administrative subpoena for Southern Kansas

Telephone Company, Inc. to identify the address. The telephone company provided the FBI with defendant's address in Howard, Kansas. Defendant's brother was the subscriber name on the internet account.[2]

On June 17, 2015, Judge Gale authorized a warrant for the FBI to search defendant's residence. Two days later, the FBI executed the search warrant and interviewed defendant at the county jail. Defendant provided a *Mirandized* confession regarding his use of Playpen and child pornography found on his devices. Approximately two years later, defendant was indicted on two counts of possession of child pornography.

II. Outrageous Conduct

Defendant asserts that the government acted outrageously when it operated Playpen without filters or limitations, thereby aiding and abetting at least 100,000 users in posting, viewing, and sharing illegal pictures and videos. Defendant is not arguing entrapment, but that the government's conduct was so inexcusable that it can only be described as outrageous.

A defendant may challenge the government's conduct during an investigation when it is sufficiently outrageous. The outrageous conduct defense is predicated on the Due Process Clause of the Fifth Amendment to the United States Constitution. If the government's conduct is deemed "outrageous," then it is not allowed to prosecute offenses developed through that conduct. The defense of outrageous conduct is distinct from the defense of entrapment, which looks at the defendant's state of mind to

[2] At the relevant time, both defendant and his brother resided with their parents in Howard, Kansas.

determine whether he was predisposed to commit the crime for which he is prosecuted. *United States v. Mosley*, 965 F.2d 906, 909 (10th Cir. 1992). In contrast, the outrageous conduct defense looks at the government's behavior. *Id.*

Other district courts have considered this claim and found that although the government's investigation and operation of Playpen had disturbing consequences, the government's conduct was not so outrageous as to warrant dismissal. *See, e.g.*, *United States v. Pawlak*, 237 F. Supp. 3d 460, 471 (N.D. Tex. 2017) (holding that the government did not violate the defendant's due process rights); *United States v. Hammond*, No. 16-CR-00102-JD-1, 2016 WL 7157762, at *6 (N.D. Cal. Dec. 8, 2016) ("While unsavory, the government's conduct did not rise to the level of outrageousness needed to support the dismissal of defendant's indictment."); *United States v. Owens*, No. 16-CR-38-JPS, 2016 WL 7079617, at *5 (E.D. Wis. Dec. 5, 2016) ("The Court is confident, however, that the government's actions in this matter were not so outrageous as to justify the dismissal of the indictment against Mr. Owens."); *United States v. Allain*, 213 F. Supp. 3d 236, 253 (D. Mass. 2016) ("Reasonable minds will no doubt differ on whether the government made the right choice here, but it is not the rare case in which any misconduct on the part of the government was sufficiently blatant, outrageous, or egregious to warrant the dismissal of the indictment.").

The court agrees with these decisions and finds that the government's conduct was not so outrageous as to support dismissing defendant's charges.

III. Motion to Suppress

Defendant challenges the initial warrant issued by the E.D. Va. magistrate,[3] and claims it was invalid under Federal Rule of Criminal Procedure 41 because it exceeded the magistrate's jurisdiction.[4]

The NIT warrant has already been subject to significant judicial scrutiny across the country. A majority of courts have found that the magistrate judge who issued the NIT warrant lacked authority to do so, yet declined to suppress the resultant evidence. *See, e.g.*, *United States v. Ammons*, No. 3:16–CR–00011–TBR–DW, 207 F. Supp. 3d 732, 2016 WL 4926438 (W.D. Ky. Sept. 14, 2016); *United States v. Henderson*, No. 15–CR–00565–WHO–1, 2016 WL 4549108 (N.D. Cal. Sept. 1, 2016); *United States v. Michaud*, No. 3:15–CR–05351–RJB, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016). A minority of district courts have suppressed evidence based on a finding that the warrant was void and the good-faith exception to the exclusionary rule did not apply. *See, e.g.*, *United States v. Levin*, No. CR 15–10271–WGY, 186 F. Supp. 3d 26, 2016 WL 2596010 (D. Mass. May 5, 2016); *United States v. Croghan*, No. 1:15–CR–48, 209 F. Supp. 3d 1080, 2016 WL 4992105

---

[3] Defendant argues that evidence from the subsequent search of his residence and his statements should be suppressed because they derived from the illegal installation of the NIT malware on his computer pursuant to *Wong Sun v. United States*, 371 U.S. 471 (1963). However, he is not directly challenging the validity of the residential warrant and interrogation.

[4] Fed. R. Crim. P. 41 has been amended and now permits magistrate judges to issue warrants such as the NIT warrant. It now reads:

> [A] magistrate judge with 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 if: (A) the district where the media or information is located has been concealed through technological means . . . .

Fed. R. Crim. P. 41(b)(6).

Because this amendment became effective on December 1, 2016, however, it does not apply to defendant's case. *United States v. Walker-Couvertier*, 860 F.3d 1, 9 (1st Cir. 2017).

(S.D. Iowa Sept. 19, 2016). But these district courts were reversed by their respective circuits, which held that the good-faith exception applied. *See, e.g.*, *United States v. Levin*, ---F.3d---, 2017 WL 4855774, at *1 (1st Cir. Oct. 27, 2017); *United States v. Horton*, 863 F.3d 1041, 1052 (8th Cir. 2017).

Recently, the Tenth Circuit bypassed directly deciding whether the E.D. Va. magistrate judge lacked authority to issue the warrant and held that even if the warrant should not have been issued, the good-faith exception to the exclusionary rule applied. *United States v. Workman*, 863 F.3d 1313, 1317, 1320–21 (10th Cir. 2017) ("[I]n our view, the executing agents acted in an objectively reasonable manner."). "Under the *Leon* exception, improperly obtained evidence remains admissible when the executing agents 'act with an objectively 'reasonable good-faith belief' that their conduct is lawful or when their conduct involves only simple, 'isolated' negligence. . . .'" *Workman*, 863 F.3d at 1317 (quoting *United States v. Leon,* 468 U.S. 897, 909 (1984) and *Davis v. United States*, 564 U.S. 229, 238 (2011)).

Defendant argues that the FBI was aware of the fact that Playpen had members throughout the world. Therefore, the executing officers knew the warrant would be invalid under the jurisdictional limitations of Rule 41 and/or the Federal Magistrates Act. Defendant contends that because "this warrant was approved at the highest levels of the FBI and the Department of Justice" the government cannot show they had a good-faith belief that the warrant was valid. (Dkt. 29, at 3).

The court finds that the E.D. Va magistrate exceeded her authority in issuing the warrant for the NIT. The court recognizes that the FBI's knowledge regarding the

validity of the warrant might cut against the government's position that the agents believed the warrant was proper. Nevertheless, the court is required to follow Tenth Circuit precedent and determines that *Workman* governs the outcome of defendant's motion. The underlying facts surrounding the E.D. Va. magistrate's authorization of the warrant and the FBI's conduct have not changed. Therefore, in accordance with *Workman*, the court finds that the good-faith exception to the exclusionary rule applies to the NIT search of defendant's computer and subsequent search of his residence.

IV. Motion for Discovery

Defendant moves for the court to order the government to provide him with a copy of the programming code for the NIT that was deployed on defendant's computer. Defendant also requests records relating to the government's review and approval of Operation Pacifier. Defendant argues that the NIT software can cause alterations in a computer's security settings permitting the computer to be exposed not only to the NIT, but to other malware or viruses that could explain why some or all of the alleged illegal materials were present on that computer. Because of this possibility, defendant requests a complete copy of NIT source code and all NIT components—including the exploit, payload server, and identifier components—used to identify Mr. Cookson's computer and any supporting documentation that could aid in understanding how the code works.

The government responds that it does not plan on using the NIT source code in its case-in-chief and further that it was not obtained from nor belonged to defendant. The government states that the NIT source code is subject to law enforcement privilege.

It also notes that the information collected by the NIT from defendant and his devices are available for defense counsel's review.

Defendant's discovery requests are denied without prejudice. All information and devices obtained from and belonging to defendant are available for review. Defendant's counsel and expert can review that information and determine whether there are materials that were not collected by and/or do not belong to defendant.

IT IS THEREFORE ORDERED this 22nd day of November, 2017, that defendant's motion to suppress (Dkt. 13) and motion to dismiss the indictment (Dkt. 14) are denied. Defendant's motion for discovery (Dkt. 15) is denied without prejudice.

s/ J. Thomas Marten
J. THOMAS MARTEN, JUDGE