19-1660-cr

United States Court of Appeals
For the Second Circuit

United States of America

Appellee,

v.

[redacted]

Defendant-Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

BRIEF FOR DEFENDANT-APPELLANT

LAW OFFICE OF
ZACHARY MARGULIS-OHNUMA
Attorneys for Defendant-Appellant
260 Madison Avenue, 17th Fl.
New York, NY 10016
(212) 685-0999

Zachary Margulis-Ohnuma
Adam Elewa
On the brief

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

Constitutional Provisions

JURISDICTIONAL STATEMENT

This court has subject matter jurisdiction pursuant to 28 U.S.C. § 1291 over the Judgment of Conviction and Sentence, A-103,[1] which was a final judgment of the United States District Court for the Eastern District of New York entered on May 29, 2019.

The Notice of Appeal, A-112, was timely filed on June 5, 2019.

ISSUE PRESENTED FOR REVIEW

The FBI seized a server in North Carolina that was distributing child pornography to users through the Dark Web, which hides the users' identities. Agents continued to operate the server in the Eastern District of Virginia. They sought permission from a Virginia magistrate judge to install software that would secretly search users' computers and transmit their personal information back to the government. The warrant application did not specify about where the searches would take place or where the targeted computers were located. The warrant itself mentioned the Eastern District of Virginia and "activating computers" but did not specify any particular location for the search. Thousands of computers around the world were searched based on the single Virginia warrant. Under these circumstances should the fruits of a search of the defendant's computer in New York based only on the Virginia warrant be suppressed?

[1] "A" refers to the Appendix filed by Defendant-Appellant.

PRELIMINARY STATEMENT

On May 23, 2019, [redacted] was sentenced to five years imprisonment based on a guilty plea to one count of receipt of child pornography, 18 U.S.C. § 2252(a). It is undisputed that all of the evidence against [redacted] was the fruit of the government's use of a "Network Investigative Technique" or "NIT", which was software that the government surreptitiously installed on [redacted] personal computer located in Queens.[2] The government used the NIT to take control of the Queens computer sometime after March 1, 2015. The NIT software then secretly transmitted [redacted] personal identifiers and other information from his computer back to the government. The NIT was triggered when [redacted] accessed Playpen, a child pornography website that the government had seized and continued to operate—*i.e.* continued to use to distribute illegal child pornography— in order to identify and prosecute its tens of thousands of users.

The government contends that this intrusion into a computer in the Eastern District of New York was authorized by a warrant issued on February 20, 2015 by a magistrate judge sitting in the Eastern District of Virginia. A prior panel of this court, confronted with three other defendants challenging similar searches based on the

[2] The term NIT is the euphemistic name given by law enforcement to computer code that breaks through the defenses of a targeted computer, takes control of the computer, and transmits information from the targeted computer back to the person who controls the NIT. Outside the law enforcement context, this code would be referred to as malware used to hack into a victim's computer. *See e.g. U.S. v. Workman*, 863 F.3d 1313, 1316 (10th Cir. 2017) (referring to NIT as "malware"); *U.S. v. Werdene*, 883 F.3d 204, 206 (3d Cir. 2018) (same).

same Virginia warrant, held that whether or not the warrant was valid or the search was lawful, the government acted in good faith and thus suppression was not warranted. *See U.S. v. Eldred*, 17-3367-cr, 2019 U.S. App. LEXIS 23294; __ F.3d __; 2019 WL 3540415 (2d Cir. Aug. 9, 2019); *see also*, *U.S. v. Scanlon*, 17-2989-cr, 2019 U.S. App. LEXIS 23283 (2d Cir. Aug. 5, 2019); *U.S. v. Allen*, 17-3154-cr, 2019 U.S. App. LEXIS 23285 (2d Cir. Aug. 5, 2019).

[redacted] respectfully submits that those holdings were erroneous. There was no ambiguity on the face of the warrant, which expressly authorized a search only in the Eastern District of Virginia. Since government agents searched in Queens, the search was clearly unauthorized. No reasonable law enforcement officer would have thought otherwise. The inquiry ought to end there. *See U.S. v. Voustianiouk*, 685 F.3d 206, 211 (2d Cir. 2012) (suppression warranted where officers searched second floor apartment even though warrant specified first floor apartment as the particular place to be searched).

However, the *Eldred* panel looked beyond the four corners of the warrant to nonetheless discern good faith by the officers based on language in the warrant *application* that was not disclosed to [redacted] until well after his arrest. But, we respectfully submit, the panel's analysis of the application was also erroneous because it overlooked the fact that language in the signed *warrant* describing the target computers—"activating computers are those of any user or administrator who

logs into the TARGET WEBSITE by entering a username and password"—*specifically omits* language in the government's warrant *application*, which had requested authorization to "cause an activating computer—*wherever located*—to send" information to the government. *See* A-73: Warrant Application at 29 (emphasis added). The magistrate judge did not sign the global warrant that the agents requested—which would have exceeded her jurisdiction—but instead signed a warrant limited to her district. Like the officers in *Voustianiouk*, the agents executing the warrant were well aware it did not authorize searches outside of the Eastern District of Virginia, and that the search of [redacted] computer in Queens was illegal.

Given the geographical limitation set forth in the warrant, coupled with the lack of particularity on the face of the warrant, high-level Justice Department attention paid to the case, misstatements made in the warrant application, a violation of Justice Department guidelines on obtaining a warrant, and the established limitations on the issuing magistrate's authority in both Fed. R. Crim. P. 41 and the Federal Magistrates Act, 28 U.S.C. § 636(a), the agents cannot be said to have acted in good faith reliance on a lawful warrant. Under the unique circumstances presented by the Playpen investigation, suppression would serve to deter future unlawful actions by law enforcement and its high cost is therefore justified.

[redacted] conviction should be reversed.

STATEMENT OF THE CASE

I. Facts from the Record Below

The basic facts in the case are set forth in two warrant applications filed in support of searches first of [redacted] personal computer, A-45 - A-77, and second of his home, A-17 - A-44.

A. The FBI takes down Playpen, a child pornography website.

In September 2014, FBI agents operating out of Maryland discovered a website called Playpen hosting large amounts of child pornography on the Tor Network, also known as the Dark Web. A-57; *see also U.S. v. Henderson*, 906 F.3d 1109, 1111 (9th Cir. 2018). Sites on the Tor network allow users to visit them "without revealing the IP address, geographic location, or other identifying information of the user's computer." *U.S. v. Henderson*, 906 F.3d at 1111. The Tor network also made it difficult for the FBI to discover the true location of Playpen and the identity of those operating it. *Id*. As of the time it was shut down, March 4, 2015, Playpen had 214,898 total members. A-23.

With help from "a foreign law enforcement agency" the FBI tracked down and seized the servers hosting Playpen at a data center in North Carolina. They identified a Florida man as the administrator operating the site. A-65 - A-66. After seizing the Playpen servers, rather than shutting down the site, the FBI made a copy and continued to operate Playpen from "a government facility" in the Eastern

District of Virginia. The government continued to publish child pornography from Playpen for 12 more days. A-66; A-23 (server was seized on February 20, 2015 and "operated in Newington, Virginia, from February 20, 2016 until March 4, 2015").

B. The government seeks a warrant in the Eastern District of Virginia permitting it to search computers accessing Playpen.

On February 20, 2015, after Playpen was relocated to the Eastern District of Virginia, the FBI sought authorization to deploy a "Network Investigative Technique" ("NIT") that it deemed "necessary . . . to locate and apprehend the TARGET SUBJECTS who are engaging in the continuing sexual abuse and exploitation of children, and to locate and rescue children from the imminent harm of ongoing abuse and exploitation." A-67. Specifically, the FBI asked the Hon. Theresa Buchanan, a magistrate judge sitting in the Eastern District of Virginia, for a warrant authorizing agents to "augment" the contents of the Playpen website "with additional computer instructions" what when downloaded from the Playpen website by a user of the site, "cause the user's activating computer to transmit certain information to a computer controlled by or known to the government." A-68. Nea the end of the government's application to use the NIT, it specifies that the "NIT may cause an activating computer—*wherever located*—to send to a computer controlled by or known to the government . . . information that may assist in identifying the computer." A-73 - A-74 (emphasis added). The government caused

Playpen to continue to distribute child pornography—and its NIT— to users around the world from the facility in the Eastern District of Virginia from February 20, 2015 until shutting it down on March 4, 2015. A-23.

C. The government installs the NIT on [redacted] computer in Queens, New York and surreptitiously transmits data back to the FBI.

Sometime between February 20, 2015 and March 4, 2015, the NIT was installed on [redacted] computer in the Eastern District of New York while he allegedly browsed the Playpen website. A-29-31. The NIT, once downloaded to [redacted] computer, caused his device to transmit identifying information to "a computer known to or controlled by the government." A-28; *see also U.S. v. Workman*, 863 F.3d 1313, 1316 (10th Cir. 2017) (diagram of how the NIT operated to identify activating computers).

According to the government, [redacted] registered the username "JIMINYCRACKET" on Playpen the same day the government took it over, February 20, 2015. A-29. Although the warrant applications are not entirely clear, it appears that FBI agents used the NIT to collect [redacted] IP address five days later, on February 25. *Id*. "JIMINYCRACKET" logged in several more times, without the IP address being revealed. A-29 - A-30. The applications do not specify whether the NIT was used to obtain other information about [redacted] computer, other than its IP address.

It is also unclear how the agents decided to target the JIMINYCRACKET account from among the more than 200,000 Playpen users. No hearing was held on the matter in this case, but one district court, summarizing transcripts from around the country, suggested that FBI agents arrogated to themselves discretion to determine which activating computers to search based on the users' observed activity on the site:

> The warrant provided that the NIT would activate "each time that any user or administrator log[ged] into Playpen by entering a username and password." (Dkt. No. 47-3 ¶ 36.) However, in practice the FBI configured the NIT to activate only when a user accessed certain posts within Playpen. Hr'g Tr. 20:19-25, *Matish*, Crim. No. 4:16-16, Dkt. No. 61 ("The way you deployed it is much narrower than what the warrant authorized, correct? [Agent Alfin answering] That is correct."). The NIT did not activate when a user reached Playpen's home page, created an account, or logged into that account. Hr'g Tr. 69:19-21, *United States v. Michaud*, Crim. No. 15-5351 (W.D. Wash. Jan. 22, 2016), Dkt. No. 203 ("THE COURT: The NIT did not just go to anyone that logged into the website? THE WITNESS [Agent Alfin]: No, your Honor. The warrant did authorize us to deploy the NIT in that fashion. [But it allowed the FBI to] restrict how we deploy the NIT, [so we] deployed it in such a fashion that the NIT was deployed against users who attempted to access illicit content."). To activate the NIT, a user actually had to access child pornography. *See, e.g.*, Hr'g Tr. 27:19-30:11, *Matish*, Crim. No. 4:16-16, Dkt. No. 61 (FBI Agent Alfin testifying the NIT only deployed when the defendant in that case sought images of bestiality involving an eleven-year-old girl); Hr'g Tr. 69:8-16, *Michaud*, Crim. No. 15-5351, Dkt. No. 203 (FBI Agent Alfin testifying the NIT only deployed when the defendant in that case sought images contained in a portion of Playpen entitled "Preteen Videos—Girls Hardcore" because "[a]t the point where a

> user in that forum accessed a post, we can affirmatively state that a user has attempted to access child pornography").

U.S. v. Knowles, 207 F. Supp. 3d 585, 593 (D.S.C. 2016).

According to the government's review of Playpen's log files, the user of the JIMINYCRACKET account was logged in for a total of 8 hours and 47 minutes between February 20 and March 1, 2015. A-29. The user accessed child pornography on Playpen's servers on February 22 and February 25, 2015. A-29 - A-30.

D. Based on the information transmitted through the NIT, agents search [redacted] home and arrest him.

The FBI issued an administrative subpoena to Time Warner to identify the physical address associated with the IP address used with the JIMINYCRACKET account. A-30. That led them to [redacted] home in Queens. A-31. On August 27, 2015, the government applied to Magistrate Judge Marilyn Go in the Eastern District of New York for a warrant to search [redacted] home. *See* A-31. The search warrant was executed on September 1, 2015. [redacted] was arrested, arraigned, and released the same day on bond. *See* ECF No. 2. The government's search of computers seized from [redacted] home uncovered various files containing child pornography. *See* ECF No. 6: Indictment dated September 30, 2015.

II. Proceedings Below

A. Suppression Motion

[redacted] filed a motion on December 2, 2016 to suppress the identifying information transmitted to the government by the NIT and the investigative fruits of that search on the grounds that the Virginia warrant was not valid and did not authorize the Queens search. ECF No. 42. [redacted] motion to suppress argued, in sum, that the NIT warrant violated both the Fourth Amendment and the federal Magistrate's Act, 28 U.S.C. § 636(a) and then-existing Fed. R. Crim. P. 41, which constitute the legislative grant of authority under which magistrate judges issue warrants. *See* ECF No. 42 at 1. [redacted] motion argued that the government's violation of these rules was not done in good faith as "no effort was made to get a proper warrant in the Eastern District of New York or in the other districts" where activating computers may have been located. ECF No. 42 at 22-24. *See also* ECF No. 52 at 1-3: 4/3/2017 Supplemental Letter re: Motion to Suppress (arguing the warrant on its face authorizes agents only to search property located within the Eastern District of Virginia and noting that the warrant failed to incorporate the affidavit that might have otherwise expanded the scope of the warrant to cover locations outside of the Eastern District of Virginia); *see also* ECF No. 61 at 4: 8/11/2017 Supplemental Letter re: Motion to Suppress (then-recent

court decisions denying suppression did not address NIT warrant's failure to incorporate affidavit).

On April 27, 2018, the district court denied [redacted] motion to suppress, holding that although the government's use of the NIT resulted in a "search" of his computer in the Eastern District of New York, and the search "violated the geographic limitations" of Fed. R. Crim. P. 41(b)(1), suppression was "not an appropriate remedy" as the government acted in good-faith reliance on the Virginia warrant. A-96-98. The district court did not address whether the NIT violated the Magistrate's Act, 28 U.S.C. § 636(a), which is the source of Rule 41's authority and contains its own territorial limits.[3]

B. [redacted] pleads guilty with a carve-out permitting this appeal.

On July 9, 2018, [redacted] pled guilty pursuant to an agreement with the government permitting him to appeal the denial of his motion to suppress. On May 23, 2019, he was sentenced to the mandatory minimum of 60 months in federal prison. *See* ECF No. 74; A-103: Judgment dated May 29, 2019. [redacted] notice of appeal was timely filed on June 5, 2019. A-9; A-112.

[3] Rule 41 has since been amended and now purports to authorize warrants like the Virginia warrant at issue here. *See* Fed. R. Crim. P. 41(b)(6) (2017). However, as is discussed below, we respectfully submit that 28 U.S.C. § 636(a), the Magistrate's Act, places a territorial limit on such warrants, restricting them to the district in which the magistrate judge sits. *See U.S. v. Eldred*, 2019 U.S. App. LEXIS 23294 at *17-18.

III. Proceedings on the NIT warrant in other cases

According to press reports and the FBI website, the FBI used the NIT to search more than 1,000 computers and has brought at least 350 cases based on those searches. FBI, *'Playpen' Creator Sentenced to 30 Years*, *available at* https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years (last accessed 9/6/2019); *see also* Petition for Initial Hearing *En Banc* filed September 6, 2019. As discussed below, while several district courts suppressed evidence obtained as a result of the NIT, those decisions have all been reversed and, to date, every court of appeals to consider the matter, including this Court, has denied suppression but no court has expressly found that the searches were lawful.

A. Four district courts suppress the fruits of the NIT warrant.

As the government started bringing dozens of Playpen cases to court in 2015 and 2016, four lower court judges who considered the matter sided with defendants aggrieved by the NIT warrant. These courts held that it was clear that the NIT search could not be authorized given the territorial restrictions on the power of the magistrate judge under 28 U.S.C. § 636(a) and Fed. R. Crim. P. 41(b), the agents did not rely on the warrant in good faith, and suppression was therefore required. *See U.S. v. Carlson*, No. 16-317 (JRT/FLN), 2017 U.S. Dist. LEXIS 67991, at *1 (D. Minn. Mar. 23, 2017) (report & recommendation); *U.S. v. Arterbury*, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091, at *35 (N.D. Okla. Apr. 25, 2016) (report

& recommendation); *U.S. v. Workman*, 205 F. Supp. 3d 1256, 1269 (D. Colo. 2016); *U.S. v. Levin*, 186 F. Supp. 3d 26, 44 (D. Mass. 2016). All were ultimately reversed under the good-faith exception to suppression articulated in *U.S. v. Leon*, 468 U.S. 897 (1984).

B. Sister circuits decline to suppress the fruit of the searches based on *Leon* good faith but criticize violations of then-existing Rule 41 and the Magistrates Act.

The circuit courts denying suppression have either assumed that the government's searches were not authorized by a valid warrant or explicitly held that the searches violated the U.S. Constitution, the Magistrates Act, 28 U.S.C. § 636(a), and Fed. R. Crim. P. 41(b). *See U.S. v. Taylor*, Nos. 17-14915, 18-11852, 2019 U.S. App. LEXIS 25950, at *2 (11th Cir. Aug. 28, 2019) (holding that government's search was without authorization, but denying suppression due to the good faith doctrine); *U.S. v. Henderson*, 906 F.3d 1109, 1114 (9th Cir. 2018), *cert. denied* 139 S. Ct. 2033 (May 13, 2019) (same); *U.S. v. Werdene*, 883 F.3d 204, 207 (3d Cir. 2018), *cert. denied* 139 S. Ct. 260 (Oct. 1, 2018) (same); *U.S. v. Workman*, 863 F.3d 1313, 1321 (10th Cir. 2017), *cert. denied* 138 S. Ct. 1546 (April 16, 2018) (same); *U.S. v. Horton*, 863 F.3d 1041, 1049 (8th Cir. 2017), *cert. denied* 138 S. Ct. 1440 (2018) (same); *see also U.S. v. Levin*, 874 F.3d 316, 321 (1st Cir. 2017) (assuming, *arguendo*, government's search was without authorization but refusing to grant suppression due to the good faith doctrine); *U.S. v. Ganzer*, 922 F.3d 579, 584 (5th

Cir. 2019) (same); *U.S. v. Moorehead*, 912 F.3d 963, 967 (6th Cir. 2019) (same); *U.S. v. Kienast*, 907 F.3d 522, 527 (7th Cir. 2018), *cert. denied* 139 S.Ct. 1639 (same); *U.S. v. McLamb*, 880 F.3d 685, 689 (4th Cir. 2018), *cert. denied* 139 S.Ct. 156 (Oct. 1, 2018) (same).

In sum, while most appellate courts appear to believe that the investigative technique used by the government to identify [redacted] violated the U.S. Constitution, 28 U.S.C. § 636(a), and Fed. R. Crim. P. 41(b), none was prepared to suppress evidence that hundreds of users accessed child pornography. Additionally, late last month one dissenting judge in the Eleventh Circuit argued in favor of suppression finding that the government did not act in good-faith reliance on the Virginia warrant. *See U.S. v. Taylor*, 2019 U.S. App. LEXIS 25950 at *29.

C. In three cases decided last month, a panel of this Court rules that the agents acted in good faith reliance on the Virginia warrant.

In August, a panel of this Court upheld convictions in three NIT cases. *See U.S. v. Eldred*, 17-3367-cr, 2019 U.S. App. LEXIS 23294; __ F.3d __; 2019 WL 3540415 (2d Cir. Aug. 9, 2019); *see also*, *U.S. v. Scanlon*, 17-2989-cr, 2019 U.S. App. LEXIS 23283 (2d Cir. Aug. 5, 2019); *U.S. v. Allen*, 17-3154-cr, 2019 U.S. App. LEXIS 23285 (2d Cir. Aug. 5, 2019). The panel set forth its reasoning in detail in *Eldred*, which held that it was unnecessary to address the defendant's "claim that the Fourth Amendment was violated by use of the NIT warrant" and that

"suppression is not warranted because the good-faith doctrine applies." *Id*. at 15, 19. In other words, the panel *assumed* the Fourth Amendment was violated by the search of Eldred's computer, but held that suppression was unnecessary because the government acted in good faith by obtaining the Virginia warrant. The panel rejected Eldred's argument that "the NIT warrant was 'facially deficient' because it—as opposed to the affidavit supporting the warrant's application—was limited to the Eastern District of Virginia and did not encompass Vermont or the many other judicial districts to which the FBI's computer instructions were delivered." *Eldred* at *15.

The panel based its conclusion on several factors:

- First, it reasoned that the affidavit supporting the warrant made clear how the NIT would work and that the search would extend beyond the Eastern District of Virginia. *Eldred* at *22.
- Second, even laying aside the affidavit, the warrant itself was clear on its face that "the place to be searched [w]as 'all activating computers,' defined in relevant part as 'any user…who logs into' Playpen." *Eldred* at *22 (emphasis by the panel).
- Third, the apparent violation of Rule 41 did not support the conclusion that the government engaged in "the sort of 'deliberate, reckless, or grossly negligent conduct' that the exclusionary rule exists to deter[,]" because the rules are unclear in light of "rapidly developing technology" and the warrant application explained how the NIT would work "in meticulous detail." *Eldred* at *23-24.

- Fourth, the panel rejected Eldred's argument that good faith should not apply because the NIT warrant was void ab initio because even if the magistrate had no power to issue the warrant in the first place, that was the magistrate's error and law enforcement reasonably relied on the warrant such that suppression would serve no deterrent purpose. *Eldred* at *25-26.

In *U.S. v. Scanlon*, 17-2989-cr, 2019 U.S. App. LEXIS 23283 (2d Cir. Aug. 5, 2019) and *U.S. v. Allen*, 17-3154-cr, 2019 U.S. App. LEXIS 23285 (2d Cir. Aug. 5, 2019), the same panel reiterated the same good-faith points it made in *Eldred*. In *Allen*, the panel further rejected the defendant's additional argument that the government acted in bad faith because it changed the suggestive logo on the first page of the Playpen site to something different by the time the defendant accessed Playpen, triggering the NIT search of his computer in Connecticut. *Id*. at *2-4.

SUMMARY OF ARGUMENT

We respectfully submit that *Eldred* was wrongly decided because the officers executing the NIT on [redacted] computer in New York could not have reasonably believed that the Virginia warrant authorized them to do so. Most importantly, the warrant *on its face* authorized searches of computers in the Eastern District of Virginia and nowhere else. In violation of Supreme Court precedent, the *Eldred* panel placed far too much weight on the warrant *application*. The panel also appears to have overlooked the fact that the application sought a broader search—for activating computers "wherever located"—than what was ultimately granted in

the warrant itself. No reading of the warrant consistent with the Supreme Court's directive in *Groh v. Ramirez*, 540 U.S. 551, 557-58, 124 S. Ct. 1284, 1289-90 (2004), (holding that a search based on an insufficiently particular warrant violates the Fourth Amendment even if the warrant *application* specified the location to be searched) could possibly authorize a search outside of the Eastern District of Virginia.

Second, any reasonably well-trained law enforcement officer would have recognized that the NIT warrant did not "particularly describe[e] the place to be searched" and thus could not constitutionally be executed absent further written instructions from the issuing magistrate. U.S. Const. Amend. IV. While there is precedent for "anticipatory searches" that are authorized once a triggering event takes place, there has never been a lawful warrant for a search that did not particularly describe the place to be searched. The NIT warrant described an event—the activation of the website—but failed to describe any place to be searched. No law enforcement officer serious about upholding the Constitution would have been satisfied with such a warrant.

Finally, as numerous commentators have concluded, good faith should not apply here because the government, in violation of its own best practices, deliberately misled the issuing magistrate about the scope of the search, where the

search would take place, and the scope of the magistrate judge's authority to authorize such a search.

We concede that the cost to society of suppression in this case is high. But the NIT warrant was so uniquely expansive, intrusive, and objectionable under the principles expressed in the Fourth Amendment that suppression would pay an important dividend by forcing the FBI to obtain a facially valid warrant before breaking into a suspect's computer. "[I]t is not asking too much that officers be required to comply with the basic command of the Fourth Amendment before the innermost secrets of one's home or office are invaded." *Berger v. New York*, 388 U.S. 41, 63 (1967). The *Eldred* panel erred by failing to suppress.

ARGUMENT

On appeal from a district court's ruling on a suppression motion, this Court reviews factual findings for clear error and "resolution of questions of law and mixed questions of law and fact *de novo*." *U.S. v. Bohannon*, 824 F.3d 242 247-48 (2d Cir. 2016). Where the defense demonstrates a violation of the Fourth Amendment and the government claims it acted in good faith, the burden is on the government to demonstrate the objective reasonableness of the officers' good faith. *U.S. v. Voustianiouk*, 685 F.3d 206, 215 (2d Cir. 2012), *citing U.S. v. George*, 975 F.2d 72, 77 (2d Cir. 1992).

I. The officers executing the warrant against [redacted] computer did not act in good faith because the warrant did not authorize a search in New York.

Both the *Eldred* panel and the district court here erred in concluding that the government conducted the initial search of [redacted] computer in good faith reliance on the Virginia warrant. As a threshold matter, there is no real dispute that executing the NIT on [redacted] computer was a Fourth Amendment search. *See* A-96 (district court holding that the "use of the Network Investigative Technique was a search"); *see generally U.S. v. Eldred*, 2019 U.S. App. LEXIS 23294 at *12-20 (assuming that use of the NIT was a search). Nor is there any real question that the search took place outside of the Eastern District of Virginia. *Id*. at *16 (assuming the magistrate lacked jurisdiction to authorize the NIT warrant to retrieve information located on computers outside the Eastern District of Virginia); *see also, e.g.*, *U.S. v. Taylor*, No. 17-14915, No. 18-11852, 2019 U.S. App. LEXIS 25950 at 814 (11th Cir. Aug. 28, 2019) ("It is undisputed, though, that the NIT warrant [application] sought authority to search for information outside the territorial confines of the Eastern District of Virginia"). The question then is whether it was objectively reasonable for government agents to believe that the Queens search was authorized by the Virginia warrant.

The *Eldred* panel incorrectly concluded that it was reasonable for law enforcement officers reading the warrant to believe that it permitted them to send

malware to Queens, execute it there, and allow it to send information obtained from the Queens computer back to Virginia. The panel based this erroneous finding in part on its conclusion that the "warrant itself does not contain clear geographic limits on the place to be searched. Quite the opposite—Attachment A to the NIT warrant refers to the place to be searched as all 'activating computers,' defined in relevant part as 'any user . . . who logs into' Playpen." *Eldred* at *21.

In focusing on the attachment, the *Eldred* panel ignored the operative language of the warrant itself, which states:

> **To: Any authorized law enforcement officer**
>
> **An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Virginia (identify the person or describe the property to be searched and give its location): See Attachment A**
>
> **The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized): See Attachment B**
>
> **I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.**
>
> **YOU ARE COMMANDED to execute this warrant on or before March 6, 2015….**

A-78: 2/20/15 Eastern District of Virginia Search Warrant.

As the *Eldred* panel noted, Attachment A describes the property to be searched as "the activating computers described…[as]…those of any user or

administrator who logs into the TARGET WEBSITE[.]" A-79. But this definition is not nearly so broad as the *Eldred* panel described it. Nowhere does the warrant say law enforcement is commanded to search *all* activating computers—and, in fact, it is unclear which computers among the thousands that logged in the government chose to search.

Moreover, while the warrant *application* asks for permission to take control of "an activating computer—wherever located[,]" the warrant itself omits the "wherever located" language. *Compare* A-73 (warrant affidavit at 29) with A-78 (warrant). That is, the government requested permission to search activating computers "wherever located" but the warrant on its face references only activating computers "located in the Eastern District of Virginia."

The language of the warrant, not the intent of the officers, controls: "In determining the permissible scope of a search that has been authorized by a search warrant, however, we must look to the place that the magistrate judge who issued the warrant intended to be searched, not to the place that the police intended to search when they applied for the warrant." *U.S. v. Voustianiouk*, 685 F.3d 206, 211 (2d Cir. 2012) (suppressing evidence where officers searched an apartment on the second floor of a building, even though the warrant authorized only a search on the first floor; no good faith because officers "knowingly ventured beyond the clear confines of their warrant"). Accordingly, even reading the warrant alongside the application,

there was no ambiguity that the authorization extended to any activating computer in the Eastern District of Virginia, not any activating computer wherever located as requested in the application.

The *Eldred* panel nonetheless reasoned that the affidavit made clear that "the search would extend beyond the boundaries of the district," which, it said, supported "the officers' good faith reliance[.]" *U.S. v. Eldred* at *21. The panel did not specify reliance on *what*: the warrant or the application? Even if the application *did* support the panel's conclusion, the panel's focus on it was a legal error because, under well-established Supreme Court precedent, the officers were not entitled to rely on the affidavit, which was not incorporated into the warrant or revealed to [redacted] until much later. As the Supreme Court explained:

> The fact that the application adequately described the "things to be seized" does not save the warrant from its facial invalidity. The Fourth Amendment by its terms requires particularity in the warrant, not in the supporting documents. And for good reason: [t]he presence of a search warrant serves a high function, and that high function is not necessarily vindicated when some other document, somewhere, says something about the objects of the search, but the contents of that document are neither known to the person whose home is being searched nor available for her inspection. We do not say that the Fourth Amendment prohibits a warrant from cross-referencing other documents. … But in this case the warrant did not incorporate other documents by reference, nor did either the affidavit or the application (which had been placed under seal) accompany the warrant. Hence, we need not further explore the matter of incorporation.

Groh v. Ramirez, 540 U.S. at 557-58 (internal quotations and citations omitted); *accord, e.g.*, *U.S. v. Galpin*, 720 F.3d 436, 448 (2d Cir. 2013).

In this case, the divergence between the warrant application and the face of the warrant undercuts any argument that officers acted in good faith reliance on a warrant when they searched [redacted] computer. The divergence between the request to search any activating computer wherever located and the authorization to search any activating computer in the Eastern District of Virginia was no mere clerical error or oversight. It goes to the heart of what the magistrate authorized and, indeed, what she had the *authority* to authorize under Fed. R. Crim. P. 41(b) and the Magistrate's Act, 18 U.S.C. 636. If indeed the officers who executed the NIT knew about the warrant application, they knew that the warrant authorized something different. If they did not know about the application, they had no cause at all to believe they were authorized to search beyond the Eastern District of Virginia.

II. The officers executing the warrant on [redacted] computer could not have relied on the warrant in good faith because it did not "particularly describe the place to be searched[.]"

The NIT warrant was also obviously defective on its face because it failed to identify any particular place to be searched, in direct contravention of the plain language of the Fourth Amendment. See *Berger v. New* York, 388 U.S. 41, 55 (1967) ("The Fourth Amendment commands that a warrant issue not only upon probable

cause supported by oath or affirmation, but also 'particularly describing the place to be searched, and the persons or things to be seized.'"). A reasonably well-trained law enforcement officer who took seriously his duty to act in conformance with the Constitution—even when it made the competitive business of ferreting out crime that much harder—would not have executed a search based on this warrant. The government did not meet its Therefore, suppression is a necessary deterrent to promote respect for the basic requirement of particularity in warrants.

The Fourth Amendment requires that a warrant "particularly describ[e]" the place to be searched and the persons or things to be seized. U.S. Const. Amend. IV. This particularity requirement arose out of the Founders' experience with abusive general warrants. *See Steagald v. U.S.*, 451 U.S. 204, 220 (1981) (purpose of Fourth Amendment was to ban writs of assistance that "left customs officials completely free to search any place where they believed [uncustomed] goods might be"); *see generally* William J. Cuddihy, The Fourth Amendment: Origins and Original Meaning 602-1791 (2009). The Fourth Amendment "specifies only two matters that must be 'particularly describ[ed]' in the warrant: 'the place to be searched' and 'the persons or things to be seized.'" *U.S. v. Grubbs*, 547 U.S. 90 (2006).

Mandating that the warrant describe "with particularity the place to be searched" protects against wide-ranging exploratory searches unsupported by probable cause. *U.S. v. Rosa*, 626 F.3d 56 (2d Cir. 2010), *quoting Maryland v.*

Garrison, 480 U.S. 79, 84 (1987). Particularity ensures "those searches deemed necessary [are] as limited as possible." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). And it prevents warrants issued on "loose" or "vague" bases. Wayne R. LaFave, Search and Seizure § 4.6(a) (4th ed. 2004), *citing Go-Bart Importing Co. v. U.S.*, 282 U.S. 344, 357 (1931).

Even read correctly to limit its application to the Eastern District of Virginia, the NIT warrant on its face authorized the search of potentially thousands of computers, including, ironically, computers in the government corridor near Washington D.C. that includes both the CIA and the NSA. The warrant application identified 158,094 total Playpen users who might be subject to the NIT search. A-57. Indeed, according to papers submitted under seal in another case, the FBI used the NIT to search and obtain IP addresses from 9,000 computers in more than 100 countries around the world. *See U.S. v. Tippens*, No. 16-05110-RJB, ECF No. 106: Order on Defendants' Motion to Dismiss Indictment at 5 (W.D. Wash. Nov. 30, 2016) (citing sealed document). Nothing in the warrant came close to authorizing such a "virtual, all-encompassing dragnet." *U.S. v. Bridges*, 344 F.3d 1010, 1016 (9th Cir. 2003).

Without identifying a particular place to be searched, *i.e.* a particular computer, the NIT warrant was little better than a writ of assistance. *See In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753,

758-59 (S.D. Tex. 2013) (denying warrant that would authorize investigators to surreptitiously install malware on a computer whose physical location was unknown because the request was not sufficiently particularized). Like the eavesdropping statute struck down in *Berger*, *supra*, the warrant fails to specify "the place to be searched." *Berger v. New York*, 388 U.S. at 56. Here, as in *Berger*, "[t]he need for particularity . . . is especially great" because a warrant authorizing the government to surreptitiously take over a person's computer "involves an intrusion on privacy that is broad in scope."

Moreover, as *amici* have pointed out in other NIT cases, the warrant could have been particularized based on further investigation. *See U.S. v. Henderson*, No. 17-10230, Brief of Amicus Curiae Electronic Frontier Foundation in Support of Defendant-Appellant at 13-15 (9th Cir. October 31, 2017). The FBI possessed the server that hosted the Playpen site and, thus, was able to monitor present and past activity *on the site*. Based on this activity, the government could track users as they posted and accessed certain information; track the frequency with which users accessed or engaged in activity on the site; and track the nature of the content specific users accessed. Armed with this information, the FBI could have sought particularized warrants based on specific facts, tied to specific users and their activity, thus authorizing searches and seizures against identified users and their computers. Additional investigative techniques were available to the government—

such as reviewing user activity on the site for evidence of users' actual locations or identities. "Yet the government chose to include none of these limiting factors." *U.S. v. Leary*, 846 F.2d 592, 604 (10th Cir. 1988). Instead, it relied on an uncabined, generic classification, "activating computers," specifying no "place to be searched" and encompassing a limitless number of computers in locations across the globe. In effect, it obtained an obviously unconstitutional general warrant rather than a particularized one. *See U.S. v. Leary*, 846 F.2d at 604-05 ("warrant is flawed because information was available to the government to make the description of the items to be seized much more particular").

III. The warrant was not obtained in good faith.

Finally, even if the Virginia warrant authorized the New York search and were sufficiently particularized, the government was not entitled to rely on it because—as almost all the other Playpen defendants have unsuccessfully argued—it was not *obtained* in good faith. The government misled the issuing magistrate judge about where the search would occur and her authority to issue the warrant. Moreover, the government knew exactly what it was doing: the highest levels of the Department of Justice and the FBI were consulted and, in fact, had recently issued a manual urging agents to get multiple warrants in precisely this situation. Accordingly, suppression is appropriate and indeed necessary to deter such government conduct in the future.

A. The government misled the magistrate judge about where the searches would occur.

As Judge Gerald Bart Tjoflat eloquently explained in dissent in *U.S. v. Taylor*, Nos. 17-14915, 18-11852, 2019 U.S. App. LEXIS 25950, at *29, *41-51 (11th Cir. Aug. 28, 2019), the agents obtaining the warrant falsely told the issuing magistrate "that the property to be searched would be 'located in the Eastern District of Virginia.'" *Id*. at *32. This is the converse of our primary argument, but still holds true: while we submit that the agents sought and obtained a warrant only for Virginia, then unlawfully searched in New York, Judge Tjoflat maintains that the agents tricked the issuing magistrate into signing a warrant that would authorize a search in New York by clouding the fact that they planned to search here.

Either way, the government acted in bad faith and the deterrence of suppression is appropriate. The warrant was not the product of a single federal agent who might have been mistaken on the law. High level justice department attorneys drafted the warrant application, including the FBI's Office of General Counsel. *See Transcript of Motion Hearing held on October 14*, 2016 at 46-47, *U.S. v. Anzalone*, No. 15-cr-10347-PBS (D. Mass. Oct. 28, 2016) (ECF No. 131) (stating that the decision to seek the NIT warrant and continue operating Playpen "was done with the approval of executives in both the FBI and the Department of Justice" including the "FBI Office of General Counsel").

Moreover, as Judge Tjoflat points out, the government was clearly aware there was a jurisdictional problem with having a NIT warrant signed by a magistrate judge because a Texas magistrate judge had in 2013 published a decision declining to authorize just such a warrant on the ground that Rule 41(b) did not grant such extraterritorial authority. See *Taylor* at *33-37, *citing In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d at 755. In response the Justice Department sought and obtained an amendment to Rule 41. *Id*. at 36-37. "The Justice Department's extensive involvement in the rule change—including the two highest ranking officials in the Criminal Division—makes it hard to accept that none of the Justice Department officials involved in the NIT warrant was aware of the jurisdictional issue." *Taylor* at 37-38.

Indeed, the agents applying for the warrant must have been aware of the jurisdictional problem that they hid from Magistrate Judge Buchanan because their own 2009 training manual, entitled *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* advised that it is appropriate to obtain multiple warrants when a network investigation might cross district lines. *See* A-93; *see also* ECF No. 62 (Letter from defense counsel to Judge Block enclosing manual excerpt). The advice is quite specific: "agents should obtain multiple warrants if they have reason to believe that a network search will retrieve data stored in multiple locations…[and] obtain additional warrants for each location where the

data resides to ensure compliance with a strict reading of Rule 41(b). For example, if the data is stored in two different districts, agents should obtain separate warrants from the two districts." A-93. It goes without saying that the agents here flagrantly flouted this advice.

B. Suppression is merited because the warrant was void *ab initio* and even if it was not, suppression would effectively deter the government's disregard for the rules under the unique circumstances present in this case.

Finally, the *Eldred* panel did not reach the question of whether the warrant was void *ab initio* because, it found, any mistake was that of the issuing magistrate and not the government agents. *See Eldred*, 2019 U.S. App. LEXIS 23294 at *25-26. We respectfully submit that to the extent the warrant could be read to extend outside the Eastern District of Virginia, it was void because it violated the territorial limits in Fed. R. Crim. P. 41(b) as they existed at the time and the Federal Magistrates Act, 28 U.S.C. 636(a). *See U.S. v. Werdene*, 883 F.3d 204, 210 (3rd Cir. 2018) ("We hold that the NIT warrant violated Rule 41(b). As a result, the magistrate judge not only exceeded her authority under the Rule as then drafted, but also under the Federal Magistrates Act, rendering the warrant void *ab initio* and raising the magnitude of the infraction from a technical one to a Fourth Amendment violation.").

This infirmity was of a constitutional dimension, prejudiced [redacted] and thus warranted suppression under *U.S. v. Burke*, 517 F.2d 377 (2d Cir. 1975) (Friendly, J.) (intentional disregard for a rule or prejudice to the defendant will justify suppression when there is an error in the execution of a warrant) and *U.S. v. Krueger*, 809 F.3d 1109 (10th Cir. 2015) (Gorsuch, J.) (suppressing fruits of an Oklahoma search based on a warrant issued by a Kansas magistrate, where 'the Oklahoma search might not have occurred" if the government had obeyed Rule 41).

Moreover, as Judge Tjoflat's dissent makes clear, the error here was a deliberate product of the government's warrant application. Thus, whether or not the Court adopts a *per se* rule that void warrants cannot be relied on under *Leon*, under the circumstances presented here, the purposes of the exclusionary rule would be served by suppression. As Judge Tjoflat explained:

> With this case, ten courts of appeals have sanctioned the following standard: When law enforcement officials apply for a warrant, even if they know the warrant is constitutionally suspect, so long as they technically disclose the facts that would reveal the problem to a discerning magistrate, no matter how cursory or buried the disclosure, the warrant is effectively unimpeachable if the magistrate fails to detect the problem. I cannot believe that the law expects so little of law enforcement, or so much of magistrates.
>
> This standard creates a warped incentive structure. It encourages law enforcement to obscure potential problems in a warrant application. Because officials can be less upfront about problems in a warrant application, the onus is on the magistrate to spot the issues. But it is well-

> established that if a magistrate makes a mistake—*e.g.*, misses an issue, gets the law wrong—that mistake will almost always be forgiven because the police can generally rely on an approved warrant in good faith. *See Leon*, 468 U.S. at 922. This is a system designed to encourage mistakes.
>
> ***
>
> I'm not advocating to change the law—the law already requires candor in warrant applications. I'm asking courts to take this requirement seriously.
>
> When the Supreme Court established the good faith exception, the principal dissent warned that it would "put a premium on police ignorance of the law." *Leon*, 468 U.S. at 955 (Brennan, J., dissenting). Justice Brennan predicted that in close cases "police would have every reason to adopt a 'let's-wait-until-it's-decided' approach in situations in which there is a question about a warrant's validity or the basis for its issuance." *Id*. With this decision, his premonition has come true.

U.S. v. Taylor, 2019 U.S. App. LEXIS 25950 at *54-57.

CONCLUSION

Because the government did not act in good faith in either obtaining or executing the NIT warrant, the judgment of the district court should be REVERSED and the case remanded for further proceedings.

Dated: New York, New York
September 6, 2019

Respectfully submitted,

Law Office of Zachary Margulis-Ohnuma

By: *Zachary Margulis-Ohnuma*
Zachary Margulis-Ohnuma
Adam Elewa
260 Madison Avenue, 17th Fl.
New York, NY 10016
(212) 685-0999

Attorneys for Appellant [redacted]

CERTIFICATE OF COMPLIANCE

I hereby certify that this brief complies with the requirements of Fed. R. App. P. 32(a)(5) and (6) because it has been prepared in a 14-point proportionally spaced font.

I further certify that this brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because it contains **8.898** words, excluding the parts of the brief exempted under Rule 32(f) according to the count of Microsoft Word.

Zachary Margulis-Ohnuma
Zachary Margulis-Ohnuma