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

PETITION FOR INITIAL HEARING *EN BANC*

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

Appellant [redacted] petitions this Court pursuant to Rule 35 of the Federal Rules of Appellate Procedure for an initial hearing *en banc*. This case should be heard *en banc* in the first instance because it involves a question of exceptional importance under Rule 35(a)(2) of the Federal Rules of Appellate Procedure. Fed. R. App. P. 35(a)(2). In addition, a panel of this Court last month issued an opinion and two orders that, we respectfully submit, conflict with a decision of the United States Supreme Court and this Court's precedents and thus rehearing is also warranted under Fed. R. App. P. 35(a)(1).

The exceptionally important question presented in this case is whether the fruits of dozens or hundreds of searches in the Second Circuit should be suppressed, where the searches were all based on a single warrant issued by a magistrate judge in the Eastern District of Virginia that did not authorize searches outside that district, did not particularly describe any place to be searched in the Second Circuit or elsewhere, and the warrant was obtained through a misleading application by government agents.

Last month, a panel of this court held that the government acted in good faith in applying for the warrant in Virginia and executing it in New York in an opinion, *U.S. v. Eldred*, 17-3367-cr, 2019 U.S. App. LEXIS 23294; __ F.3d __; 2019 WL 3540415 (2d Cir. Aug. 9, 2019), and two summary orders, *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). As is discussed in detail in our Brief for Defendant-Appellant ("Br."), which is being filed simultaneously herewith, the panel's opinion conflicted with the Supreme Court decision in *Groh v. Ramirez*, 540 U.S. 551, 557-58 and this court's earlier opinion in *U.S. v. Galpin*, 720 F.3d 436, 448 (2d Cir. 2013) inasmuch as it effectively relied on an unincorporated, unattached and secret warrant affidavit to justify a search that was not authorized by the warrant itself. *See* Br. at 19-23.

FACTUAL BACKGROUND

On May 23, 2019, appellant [redacted] was sentenced to five years imprisonment based on a guilty plea to one count of receipt of child pornography under 18 U.S.C. § 2252(a). A-103: Judgment dated 5/29/2019.[1] The evidence against Mr. [redacted] consisted entirely of the fruit of the government's use of a "Network Investigative Technique" or "NIT", which was software that the government surreptitiously installed on Mr. [redacted] personal computer located in Queens. *See* A-29 – A-30 (New York search warrant application for [redacted] residence based on information obtained from the NIT). Sometime after February 20, 2015, the government used the NIT to secretly transmit Mr. [redacted] personal identifiers and other information from his computer back to

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

the government. *Id*. 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. *Id*. Altogether, the NIT was used to search about 9,000 computers in more than 100 countries around the world, including 2,000 computers in the United States. *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).

Based on the information obtained through the NIT, the government applied for a warrant to search Mr. [redacted] residence, where agents found additional evidence that Mr. [redacted] had possessed child pornography.

PRIOR PROCEEDINGS

In a motion to suppress and subsequent filings in the district court, Mr. [redacted] challenged the initial search of his computer in Queens on Fourth Amendment grounds, arguing, *inter alia*, that the Virginia warrant on its face did not grant the agents authority to search his New York computer; that the warrant failed to particularly identify the place to be searched; that even if the warrant was facially valid, it violated the territorial restrictions found in Rule 41 of the Federal Rules of Criminal Procedure and the Federal Magistrates Act, 18 U.S.C. § 636 and that these

violations were of a constitutional dimension and prejudiced Mr. [redacted] rendering the warrant invalid and suppression required.

The district court, following the approach of many courts around the country, denied Mr. [redacted] motion to suppress. It held that the government's use of the NIT resulted in a "search" of Mr. [redacted] computer in the Eastern District of New York, and that the search "violated the geographic limitations" of Fed. R. Crim. P. 41(b)(1), but that suppression was not appropriate since the government acted in good-faith reliance on the Eastern District of Virginia warrant. A-96 – A-98.

In August, a panel of this Court upheld convictions in three cases involving additional defendants whose computers had been searched using the NIT relying on the same Virginia warrant. *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 the *Eldred* opinion, 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." *U.S. v. Eldred*, 2019 U.S. App. LEXIS 23294 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. In determining that suppression was not warranted, the panel relied on the warrant affidavit to conclude that the officers acted in good faith because a "reasonable reader would have understood that the search would extend" outside the Eastern District of Virginia even though the application was not incorporated or attached to the warrant. *Id*. at *21-22.

An unknown number of additional NIT cases have been brought in the district courts of the Second Circuit and may make their way to this court.

ARGUMENT

Initial hearing *en banc* is appropriate here because the question of good faith raised by the NIT warrant is exceptionally important and the *Eldred* panel answered it incorrectly.

A. The good faith question raised here affects thousands of pending and future cases.

The question of whether the good faith exception to the exclusionary rule articulated in *U.S. v. Leon*, 468 U.S. 897 (1984), applies here is exceptionally important because it not only directly affects what may turn out to be dozens of NIT cases brought in this Circuit, but also the possibly thousands of individuals searched by the NIT already as well as countless additional cases that law enforcement could

bring if permitted to routinely flout the Constitution under the guise of good faith. *See U.S. v. Taylor*, Nos. 17-14915, 18-11852, 2019 U.S. App. LEXIS 25950 at *29, *47-59 (11th Cir. Aug. 28, 2019) (Tjofat, J., dissent) ("[T]he law enforcement officials who sought the warrant…knew or should have known that there was an issue with jurisdiction and that the search would occur outside the district. Yet, the officials told the magistrate repeatedly that the search would take place in the district. If the law condones this conduct, it makes a mockery of the warrant process."). This single case will determine the consequences of the government purporting to rely on a single warrant to run an international dragnet, breaking into "thousands of computers in 120 countries," most of which were hundreds of miles outside of the issuing district. *See U.S. v. Carlson*, No. 16-317 (JRT/FLN), 2017 U.S. Dist. LEXIS 67991, at *10 (D. Minn. Mar. 23, 2017); *see also Order on Defendants' Motion to Dismiss Indictment* at 5, *U.S. v. Tippens*, No. 16-05110-RJB (W.D. Wash. Nov. 30, 2016) (ECF No. 106) (estimating that the government searched nine thousand computers, seven thousand of which were located outside of the United States).

Notably, not a single appellate court, including the Second Circuit, has found that the Virginia warrant *actually* authorized the government to search computers outside of Virginia. S*ee* Br. at 13-14. Nor does any circuit court gainsay that the malicious software distributed by the government—the NIT—effectuated a search under the Fourth Amendment, or that the search occurred where the defendant was

located, rather than the location of the server in Virginia. *Id.* The government, therefore, carried out thousands of searches in nearly every district in the United States with only a single Virginia magistrate reviewing the legality of the government's search prior to its execution.

The media, legal commentators, and non-profit organizations have recognized the importance of this case and weighed in, almost universally supporting defendants seeking suppression of material obtained through what they see as a clear-cut case of the government using invasive, illegal hacking tools not available to law-abiding citizens. The majority of appellate cases have entertained carefully thought out *amicus* briefs. *See, e.g., U.S. v. Horton*, 16-3976, ECF No. 4487708, *Brief of Amicus Curiae Electronic Frontier Foundation in Support of Defendants-Appellees and Affirmance* (8th Cir. Jan. 9, 2017); *U.S. v. Levin*, 16-1567, ECF No. 00117117816, *Brief of Amicus Curiae Privacy International in Support of Defendant-Appellee and in Support of Affirmance of the Decision Below* (1st Cir. Feb. 14, 2017); *U.S. v. Workman*, 16-1401, ECF No. 01019781400, *Brief of Amicus Curiae Electronic Frontier Foundation in Support of Defendant-Appelle and Affirmance* (10th Cir. March 15, 2017); *U.S. v. Werdene*, 16-3588, ECF No. 003112605572, *Brief of Amicus Curiae Privacy International in Support of Appellant and in Support of Reversal of the Decision Below* (3rd Cir. April 26, 2017); *U.S. v. Eure*, 17-4167, ECF No. 15-1, *Brief of Amicus Curiae Privacy International in Support of Appellant and*

Reversal (4th Cir.), May 18, 2017; *U.S. v. McLamb*, 17-4299, ECF No. 18, *Brief of Amici Privacy International in Support of Appellant and Reversal* (4th Cir. June 27, 2017); *U.S. v. Kienast*, 17-1840, ECF No. 40, *Brief of Amici Curiae Electronic Frontier Foundation*, *American Civil Liberties Union Foundation, ACLU of Wisconsin, Inc. and the National Association of Criminal Defense Lawyers in Support of Defendant-Appellant* (7th Cir. Sept. 12, 2017); *U.S. v. Henderson*, 17-10230, ECF No. 16, *Brief of Amici Curiae American Civil Liberties Union, ACLU of Northern California, ACLU of Arizona, ACLU of Hawai'i & ACLU of Oregon in Support of Defendant-Appellant* (9th Cir. Oct. 31, 2017). Academics[2] and news organizations[3] have also criticized the breathtaking scope of the FBI's use of the NIT.

---

[2] *See e.g. Ahmed Ghappour, Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web, U.C. Hastings Legal Res. Paper No. 170 (2016); Steven M. Bellovin et al., Insecure Surveillance: Technical Issues with Remote Computer Searches, Computer, Mar. 2016,https://www.computer.org/cms/Computer.org/ComputingNow/issues/2016/06/mco2016030014.pdf; Susan W. Brenner, Zach Lerner, A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure, 18 Yale J.L. & Tech. 26 (2016).*

[3] *See e.g.* Joseph Cox, *The FBI Hacked Over 8,000 Computers In 120 Countries Based on One Warrant*, Motherboard, Nov. 22, 2016, https://motherboard.vice.com/read/fbi-hacked-over-8000-computers-in-120- countries-based-on-one-warrant; Kim Zetter, *Everything We Know About How the FBI Hacks People*, Wired, May 15, 2016, *available at* https://www.wired.com/2016/05/history-fbis-hacking (last visited September 6, 2019); Kevin Poulsen, *Visit the Wrong Website, And The FBI Could End Up In Your Computer*, Wired, Aug. 5, 2014, http://www.wired.com/2014/08/operation_torpedo (last visited September 6, 2019); Michael Nunez, *FBI Drops All Charges in Child Porn Case to Keep Sketchy Spying Methods Secret*, Gizmodo, Mar. 6, 2017, http://gizmodo.com/fbi- drops-all-charges-in-child-porn-case-to-keep-sketch-1793009653 (last visited September 6, 2019); Cyrus Farivar, *After FBI Briefly Ran Tor-Hidden Child-Porn Site, Investigations Went Global*, Ars Technica, Jan. 22, 2016; Ellen

The question of whether the government acted in good faith, therefore, comes before this Court accompanied by overwhelming support for the conclusion that the government acted without legal authority, and in manner that was sweeping, unprecedented, and at the very least troubling to both members of the judiciary and legal analysts. For these reasons, the underlying issue in this appeal, whether the government acted in good-faith reliance on the Virginia warrant, involves a question of exceptional importance that this Court should consider initially *en banc.*

In addition, this appeal presents an opportunity for a the Court to provide a second review of the government's search and ensure that future government investigations by the government planned and executed outside of the Second Circuit—yet designed to intrude upon the privacy of citizens within the Second Circuit—are done in good faith reliance on sufficiently particularized and clear search warrants. By hearing this appeal *en banc*, the Court can provide definitive guidance as to the geographical reach of district courts issuing warrants and the

---

Nakashima, *This Is How the Government Is Catching People Who Use Child Porn Sites*, Wash. Post, Jan. 21, 2016; Jennifer Stisa Granick, *American Spies: Modern Surveillance, Why You Should Care, and What to Do About It* (2017).

requirements of the Fourth Amendment's particularity clauses as applied to computers.

B. The *Eldred* decision conflicts with Supreme Court authority requiring officers executing a search to rely on a warrant, not on supporting documents unavailable to the person searched.

In addition, the Second Circuit's ruling in *Eldred* is based in part on a misapplication of Supreme Court precedent. *See* Fed. R. App. P. 35 (a)(1) (*en banc* favored to "secure or maintain uniformity of the court's decisions"). Specifically, the panel in *Eldred* placed too much weight on the warrant *application* in reasoning that the agents executed the *warrant* in good faith. *See* Br. at 19-23. The panel's reliance on the warrant application to support its finding of good faith conflicts with the Supreme Court's directive in *Groh v. Ramirez*, that the "Fourth Amendment by its terms requires particularity in the warrant, not in the supporting documents." *Groh v. Ramirez*, 540 U.S. 551, 557 (2004). While the Second Circuit has previously qualified this rule, allowing courts to use "unincorporated, unattached supporting documents" to factor into a determination of whether the officers acted in good faith *U.S. v. Rosa*, 626 F.3d 56, 64 (2d Cir. 2010), the panel decision in *Eldred* goes too far. In effect, it vitiates the requirement that the warrant itself state the place to be searched with particularity. To let the warrant application inform an executing agent's understanding of the scope of the warrant, documents that in this case contain conflicting descriptions of where the search would ultimately take place, would

essentially collapse the distinction between the warrant application—what the government hopes to get authority to do—and the warrant itself—which dictates the actual authority granted by a neutral and detached magistrate. This outcome is at odds with *Groh v. Ramirez* and should not be abided by this Court.

CONCLUSION

For the foregoing reasons, the petition for initial hearing *en banc* should be GRANTED.

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. 35(b)(2)(A) because it contains **2,661** 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