NO. 16-3588

IN THE UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

UNITED STATES OF AMERICA,

PLAINTIFF-APPELLEE,

V.

GABRIEL WERDENE,

DEFENDANT-APPELLANT.

On Appeal from the United States District Court
for the Eastern District of Pennsylvania
Case No. 2:15-cr-00434

The Honorable Gerald J. Pappert, United States District Court Judge

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION AND AMERICAN CIVIL LIBERTIES UNION OF PENNSYLVANIA IN SUPPORT OF DEFENDANT-APPELLANT AND REVERSAL

Andrew Crocker
Counsel for Amici Curiae
Mark Rumold
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Email: andrew@eff.org
Telephone: (415) 436-9333

Witold J. Walczak
AMERICAN CIVIL LIBERTIES UNION OF PENNSYLVANIA
247 Fort Pitt Blvd.
Pittsburgh, PA 15222
Telephone: (412) 681-7736

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rules of Appellate Procedure 26.1 and 29(a)(4)(A), amici curiae state that they do not have a parent corporation and that no publicly held corporation owns 10% or more of their stock.

Pursuant to Federal Rule of Appellate Procedure Rule 29(a)(4)(E), amici curiae certify that no person or entity, other than amici, their members, or their counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

Constitutional Provisions

STATEMENT OF INTEREST[1]

Amicus curiae Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world since 1990. With nearly 36,000 active donors, EFF represents technology users' interests in court cases and broader policy debates involving the Fourth Amendment and its relationship to technology and new surveillance techniques. Relevant here, EFF has participated as amicus before the First, Eighth and Tenth Circuits and several district courts in cases arising from the same investigation at issue in this case. *See United States v. Levin*, 16-1567 (1st Cir.); *United States v. Croghan*, Nos. 16-3976, 16-3982 (8th Cir.); *United States v. Workman*, No. 16-1401 (10th Cir.); *United States v. Matish*, No. 16-cr-0016 (E.D. Va.); *United States v. Owens*, 16-cr-0038 (E.D. Wisc.).

Amicus curiae American Civil Liberties Union of Pennsylvania is a nonprofit, nonpartisan organization with 52,000 current members. The ACLU of Pennsylvania is the state affiliate of the American Civil Liberties Union, founded in 1920 to protect and advance civil liberties throughout the United States through advocacy, public education, and litigation. The ACLU promotes the constitutional and democratic values of free expression, privacy, and liberty in a digital world. As part of this effort, its attorneys have filed numerous amicus briefs and briefs on

[1] Pursuant to Federal Rule of Appellate Procedure 29(a)(2), no party opposes the filing of this brief.

behalf of parties in cases involving electronic surveillance and privacy issues including *Riley v. California*, 134 S. Ct. 2473 (2014) (amicus); *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013) (counsel for appellee); and *United States v. Jones*, 132 S. Ct. 945 (2012) (amicus).

INTRODUCTION

This appeal—among the first of its kind—centers on a relatively new law enforcement surveillance technique: "hacking" citizens' electronic devices. More fundamentally, the case concerns what limits the Fourth Amendment places on this new technique.

Here, the government used malware (what it euphemistically calls a "NIT") to remotely hack into unknown computers, located in unknown places, in states across the country, and countries around the world. The government did this thousands of times.

All of this was done based on a single warrant.

No court would seriously consider a comparable warrant in the physical world. A warrant that authorized the search of nine thousand homes in states across the country without identifying any specific home or its location would be rejected out of hand—*even if* those searches were limited to identifying the person residing there. No principled basis exists to allow such a warrant in the digital context.

Instead of obtaining a narrowly tailored warrant, aimed at identifying particular individuals, based on specific and particularized showings of probable cause, the government sought—and received—authorization to cast its electronic net as broadly as possible.

But the breadth of that net runs afoul of the Fourth Amendment, which

"reflect[s] the determination of those who wrote the Bill of Rights that the people of this new Nation should forever 'be secure in their persons, houses, papers, and effects' from intrusion and seizure by officers acting under the unbridled authority of a general warrant." *Stanford v. Texas*, 379 U.S. 476, 481 (1965).

The warrant in this case was a general one, and it therefore violated the Fourth Amendment.

The warrant failed for an additional reason: it violated the safeguards required by Rule 41 of the Federal Rules of Criminal Procedure, as that rule stood at the time of the search. The government's malware was not a "tracking device," and it was not installed in the Eastern District of Virginia. Consequently, the magistrate who issued the warrant lacked the authority to do so.

FACTUAL BACKGROUND

This case, like hundreds of others across the country, stems from the FBI's investigation of "Playpen," a website hosting child pornography.

The FBI investigation involved hacking into "approximately nine thousand" computers in states across the country and "more than one-hundred countries" around the world—all based on a single warrant issued by a magistrate in the Eastern District of Virginia.[2]

[2] *See* Order on Defendants' Motion to Dismiss Indictment at 5, *United States v. Tippens*, No. 16-05110-RJB (W.D. Wash. Nov. 30, 2016) (ECF No. 106)

The Playpen investigation began with a tip from a foreign government. *See* Warrant Aff., ¶ 28.[3] Based on this tip, the FBI obtained a warrant and seized the servers that hosted Playpen in January 2015. *Id*. Once in physical possession of the servers, the FBI assumed the role of website administrator. *Id*., ¶ 30. During that time, it had access to all the data and other information on the server, including a list of registered users, as well as logs of their activity on the site. *Id*., ¶¶ 29, 30, 37.

A. Tor.

To access Playpen, visitors were required to use privacy-enhancing technology known as "Tor."

Tor (short for "The Onion Router") was developed to allow users to circumvent restrictions on speech and evade pervasive Internet surveillance. Tor is used by journalists, human rights advocates, lawyers, and governments—including the federal government.[4]

("*Tippens* Order").

[3] The warrant, its two incorporated attachments, and the warrant application submitted by FBI Special Agent Douglas Macfarlane, were filed under seal here, JA104-140, but are publicly available as an addendum to the government's opening brief in *United States v. Workman*, No. 16-1401 (10th Cir.). References herein to the "Warrant," "Warrant Attach." or the "Warrant Aff." are to those documents, respectively.

[4] Tor began as a project of the United States Naval Research Lab in the 1990s. *See* Tor Project, Inception, https://www.torproject.org/about/torusers.html. Recognizing the privacy-enhancing value of the technology, amicus EFF provided financial support for Tor in 2004 and 2005. *See* Tor Project, Sponsors, https://www.torproject.org/about/sponsors.html.en. The Tor Project is now an independent non-profit. *Id*.

Tor consists of a computer network and software that work together to provide Internet users with anonymity. Tor obscures aspects of how and where its users access the Internet, allowing them to circumvent software designed to censor content, avoid tracking of their browsing behaviors, and facilitate other forms of anonymous communication.[5]

The Tor network consists of volunteer-operated computers, known as "nodes" or "relays," which enable Tor users to connect to websites "through a series of virtual tunnels rather than making a direct connection."[6] To connect to the Tor network, users download and run Tor software on their devices. This software allows users to share information over public Internet networks without compromising their privacy.

Using Tor, individuals can also host websites known as "hidden services," which do not reveal the network location of the site.[7] Other Tor users can connect to hidden services without knowing the site's actual address and without the site knowing information about visitors—including information that would ordinarily be disclosed in the course of web browsing, like the Internet Protocol (IP) address assigned to users by their Internet Service Provider (ISP).

---

[5] *See* Tor Project, Inception, https://www.torproject.org/about/torusers.html

[6] *Id*. For a visual representation of how Tor works to protect web traffic, *see Tor and HTTPS*, EFF, https://www.eff.org/pages/tor-and-https.

[7] *See* Tor: Hidden Service Protocol, https://www.torproject.org/docs/hidden-services.html.

Playpen operated as a Tor hidden service. Warrant Aff., ¶ 11.

B. The FBI's use of malware.

During the two-week period the government operated Playpen, investigators used malware, which they called a "Network Investigative Technique" (NIT), to infect the computers of users logging into the site. *United States v. Levin*, 186 F. Supp. 3d 26, 30 (D. Mass. 2016). The malware allowed the government to circumvent and defeat the anonymity features of Tor by searching infected computers for identifying information about the computer and relaying that information back to the FBI. *Id*.

Malware is short for "malicious software" and is typically used as a catchall term to refer to any software designed to disrupt or damage computer operations, gather sensitive information, gain unauthorized access, or display unwanted advertising.[8]

The government developed the malware in this case and coined the term "Network Investigative Technique" or "NIT" to describe it. As a technical matter,

[8] *See* Robert Moir, *Defining Malware: FAQ*, Microsoft TechNet (Oct. 2003), https://technet.microsoft.com/en-us/library/dd632948.aspx. The term is defined by the U.S. National Institute of Standards and Technology as "a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system." Murugiah Souppaya & Karen Scarfone, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, NIST Special Publication (July 2013), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

there is little difference between a NIT and malware used by identity thieves or other criminal "hackers."[9]

The FBI's use of the NIT followed a multistep process:

1. Exploit and Delivery. The FBI's operation and control of the Playpen server allowed it to reconfigure the site to deliver its malware to visitors. *See* Warrant Aff., ¶¶ 32, 33.

To successfully deliver the malware to a target computer, the NIT relied on an "exploit," which took advantage of an unknown, obscure, or otherwise unpatched vulnerability in software running on the target computer.[10] Thus, computer code served by the government to the target computers used one or more vulnerabilities in users' software to surreptitiously deliver and install the NIT.

2. Payload. Once resident on a target computer, malware like the NIT downloads and executes a "payload"—software that allows an attacker to control a device or extract data without the knowledge or consent of the computer's owner.[11]

In the case of the government's NIT, the payload searched a user's computer and copied data from that computer. In particular, the payload accessed data that

---

[9] The NIT is similar to a class of malware known as a Remote Access Trojan ("RAT"), which often includes keystroke logging, file access and remote control, including control of microphones and webcams. *See* Roger A. Grimes, *Danger: Remote Access Trojans*, Microsoft TechNet (Sept. 2002), https://technet.microsoft.com/en-us/library/dd632947.aspx.

[10] *See Malware Protection Center*, Microsoft, https://www.microsoft.com/en-us/security/portal/mmpc/threat/exploits.aspx

[11] *See* Grimes, *supra* n.8.

would not typically be disclosed to operators of a website on the Tor network.

3. Exfiltration of Data to the FBI. The NIT then transmitted the copied information back to the FBI. The warrant authorized the collection of the following information: (1) the computer's actual IP address; (2) a unique identifier to distinguish the data from that of other computers; (3) the computer's operating system; (4) information about whether the NIT had already been delivered to the computer; (5) the computer's "Host Name"; (6) the computer's active operating system username; and (7) the computer's "Media Access Control" (MAC) address. *See* Warrant Attach. B.

The information in the NIT's transmission, as well as the associated IP address, formed the basis for all further investigation in these cases. Ultimately, the FBI searched nearly 9,000 computers, located in over 100 countries around the world in the manner described.[12]

ARGUMENT

The warrant used in this case is invalid for two reasons.

First, the warrant was an unconstitutional general warrant because it lacks the careful tailoring and particularity the Fourth Amendment requires. On its face,

[12] *Tippens* Order at 5; *see* 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.

the warrant—which did not describe any particular person or place—authorized the search and seizure of hundreds of thousands of computers located around the world. And in practice, the FBI relied on the warrant to search nearly 9,000 computers located in 120 different countries. Those facts, alone, are sufficient to render the warrant invalid.

Second, as the court below and, indeed, the overwhelming number of district courts to consider the issue have correctly held: the warrant also violated Rule 41 of the Federal Rules of Criminal Procedure because the warrant authorized searches in unknown places outside the issuing magistrate's jurisdiction.

I. THE WARRANT LACKED PARTICULARITY AND WAS THEREFORE INVALID.

The Fourth Amendment requires a warrant to "particularly describ[e]" the places to be searched and the persons or things to be seized. U.S. Const. amend. IV.

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. United States*, 282 U.S. 344, 357 (1931)). The "uniformly applied rule is that a search conducted pursuant to a warrant that fails to conform to the particularity requirement of the Fourth Amendment is unconstitutional." *Groh v. Ramirez*, 540 U.S. 551, 559-60

(2004) (internal quotations and citations omitted).

As explained below, the warrant lacked particularity, and the searches it authorized were therefore unconstitutional.

A. The warrant failed to particularly describe what was being searched and where those searches would occur.

Warrants "are fundamentally offensive to the underlying principles of the Fourth Amendment when they are so bountiful and expansive in their language that they constitute a virtual, all-encompassing dragnet[.]" *United States v. Bridges*, 344 F.3d 1010, 1016 (9th Cir. 2003).

Such is the case here: the government obtained a single warrant that, on its face, authorized the search of over 150,000 electronic devices located all over the world. Relying on the warrant, the FBI actually searched nearly 9,000 computers in over 100 different countries. That is the definition of a "virtual, all-encompassing dragnet" prohibited by the Fourth Amendment.

1. A single warrant to search 150,000 electronic devices, without specifying the location of a single one of them, fails the test of particularity. A valid warrant requires identification and description of a particular place to be searched and the particular person or thing to be seized. U.S. Const. amend. IV; *United States v. Christine*, 687 F.2d 749, 752-53 (3d Cir. 1982). Each person or place to be searched requires specific description in the warrant—accompanied by individualized probable cause—such that "the executing officer can with

reasonable effort identify the precise place

intended." *United States v. Busk,* 693 F.2d 28, 30 (3d Cir. 1982). "Where the standard is probable cause, a search or seizure of a person must be supported by probable cause particularized with respect to that person." *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979); *see also Steagald v. United States*, 451 U.S. 204, 220 (1981) (warrant to arrest a specific individual is not sufficiently particularized to give officers the "authority to enter the homes of third parties"). Ultimately, particularity "serves to limit the scope of the intrusion." *Christine*, 687 F.2d at 756.

The breadth of the warrant here, coupled with the absence of specific information about the places to be searched, rendered it invalid.

The warrant did not identify any particular person or thing to search; nor any specific user of the targeted website; nor group of particular users. It did not identify any particular device to be searched, or even a particular *type* of device. Instead, it broadly encompassed the computer of *any* visitor to the site—a category that, at the time of issuance, encompassed over 150,000 registered accounts. *See* Warrant Aff., ¶ 11.

Compounding matters, the warrant failed to provide any specificity about the actual place to be searched—the location of "activating computers." *See* Warrant Attach. A. Instead, the warrant authorized search of "any" activating computer, no matter where that computer might be located. Because an activating computer

could be located anywhere, the warrant, on its face, authorized FBI searches and seizures in every U.S. state and territory, indeed anywhere in the world.[13] As one court explained, "the NIT warrant lacks particularity because it is not possible to identify with any specificity, which computers, out of all of the computers on earth, might be searched pursuant to this warrant." Report & Recommendation at 23, *United States v. Carlson*, No. 16-cr-317 (D. Minn. Mar. 23, 2017) (ECF No. 44) ("*Carlson* R&R"); *see also In re Warrant to Search a Target Computer*, 958 F. Supp. 2d 753, 759 (S.D. Tex. 2013) (application to use NIT to identify computer in unknown location not sufficiently particular).

2. The absence of particularity was not compelled by the technology at issue. Although particularity is context-dependent and the specificity required in a warrant will vary, this Court has held that the warrant application must be as particular "as the information available would allow." *United States v. Am. Investors of Pittsburgh, Inc.*, 879 F.2d 1087, 1106 (3d Cir. 1989) (citing *United States v. Leary,* 846 F.2d 592 (10th Cir. 1988)). Indeed, "warrants are conclusively invalidated by their substantial failure to specify as nearly as possible the distinguishing characteristics" of the places to be searched and the items to be seized. *Leary,* 846 F.2d at 600 (internal quotations and citations omitted). Although

[13] *Tippens* Order at 5. The government's decision to conduct these searches—and the magistrate's decision to authorize them—raises special considerations for extraterritorial searches. *See Microsoft Corp. v. United States*, 829 F.3d 197, 212 (2d Cir. 2016).

warrants may describe items in broad or generic terms, "generic classifications in a warrant are acceptable only when a more precise description is not possible." *United States v. Bright*, 630 F.2d 804, 812 (5th Cir. 1980).

Here, *far* more precision was possible.

The FBI possessed the server that hosted the site and, thus, had a clear window into users' activities. Based on this activity, the government could track: (1) which users were posting and accessing specific information; (2) the frequency with which those users did so; and (3) the nature of the information they posted or accessed.

Using this information, the FBI could have sought warrants based on *specific* facts, tied to *specific* users and their activity, thus authorizing searches and seizures against those specific, identified users and their specific computers. Indeed, in this case, the government observed activity associated with a specific username before deploying its malware, information that easily could have been included in a warrant application. *United States v. Werdene*, 188 F. Supp. 3d 431, 438-39 (E.D. Pa. 2016).

The government could have done more still—such as reviewing user activity on the site for evidence of users' actual locations or identities. Although the true physical location of these specific users may still have been unknown, inclusion of these facts, based on specific probable cause determinations, would have

substantially narrowed the warrant.

"Yet the government chose to include none of these limiting factors." *Leary*, 846 F.2d at 604. Instead, it relied on a generic classification, "activating computers," to describe the place to be searched—a description that encompassed any computer tied to one of the 150,000 registered accounts or any future registered account.

Thus, it is by no means "immaterial" that the government could have provided additional detail in its application, thereby narrowing the scope of the warrant. *United States v. Matish*, 193 F. Supp. 3d. 585, 609 (E.D. Va. 2016). It is the difference between a single warrant to search thousands of computers, and a warrant to search individual computers based on individualized showings of probable cause. It is the difference between a general warrant and a particularized one.

Here, "circumstances permit[ted]" the government to submit more particular information; it was thus required to do so. *Leary,* 846 F.2d at 600.

B. Particularity was critical given the series of invasive searches and seizures carried out each time the malware was deployed.

Using malware to control private computers and copy private information is an invasive surveillance technique—an invasion glossed over by the government's description of its malware as mere "computer instructions." Warrant Aff., ¶ 33.

Each use of the malware triggered three Fourth Amendment events: (1) an

entry into and seizure of a user's computer; (2) a search of the private areas of that computer; and (3) a seizure of private information from the computer.

Given the significant Fourth Amendment events that occurred each time the government deployed its malware, a specific and particularized warrant was crucial. But the warrant was not limited to a single search or seizure or to a single user. Rather, on its face, the warrant authorized the FBI to repeatedly execute these invasive searches and seizures—upwards of hundreds of thousands of times.

1. The government's malware exploited an unpatched vulnerability in software running on a user's computer, turning the software against the user—and into a law enforcement investigative tool. This is a Fourth Amendment seizure.

A seizure occurs when "there is some meaningful interference with an individual's possessory interests" in property. *United States v. Jacobsen,* 466 U.S. 109, 113 (1984).

Here, users undeniably have possessory interests in their personal property—their computers and the private information stored on those computers. The government interfered with those possessory interests when it surreptitiously placed code on the computers. Even if the malware did not affect the normal operation of the software, it added a new (and unwanted) feature—it became a law enforcement tool for identifying Tor users. This exercise of "dominion and control," even if limited, constitutes a seizure. *See id*. at 120-21 & n.18; Report and

Recommendation at 11-12, *United States v. Arterbury*, 15-cr-0018 (N.D. Ok. filed Apr. 25, 2016) (ECF No. 42); *cf. United States v. Jones*, 565 U.S. 400, 404 (2012) (Fourth Amendment search occurred where "government physically occupied" individual's property by affixing GPS tracker to it).

2. The government's malware operated by seeking out certain information stored on affected computers. This is a Fourth Amendment search.

A search occurs when the government infringes on an individual's "reasonable expectation of privacy." *Katz v. United States*, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring).

Individuals have a reasonable expectation of privacy in their computers and private information stored therein. Computers "are simultaneously offices and personal diaries" and "contain the most intimate details of our lives." *United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013). As the Supreme Court recognized in *Riley v. California*, due to the wealth of information that electronic devices "contain and all they may reveal, they hold for many Americans 'the privacies of life.'" 134 S. Ct. at 2494-95 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)). Thus, a user's personal computer is a private area subject to the user's reasonable expectation of privacy.

A search that occurs inside a person's home, on their personal computer, must be provided the Fourth Amendment's highest protection. It is no surprise,

then, that courts uniformly recognize the need for warrants prior to searching computers. *See, e.g.*, *United States v. Stabile*, 633 F.3d 219, 232 (3d Cir. 2011); *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001); *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007).

In this case, a search occurred because the government's malware operated directly on users' computers. The malware "searched" the device's memory for information stored on the computer. *See* Warrant Aff., ¶ 33. Nothing more is necessary to give rise to a Fourth Amendment interest. *See Rakas v. Illinois*, 439 U.S. 128, 143 (1978).

Nevertheless, the district court below improperly focused on the *information obtained* from the search rather than *the place where the search occurred*. The court incorrectly concluded no Fourth Amendment search occurred because "Werdene had no reasonable expectation of privacy in his IP address." *Werdene*, 188 F. Supp. 3d at 444. But this holding relies on *Smith v. Maryland*, 442 U.S. 735 (1979), and its progeny, which involved warrantless access to information in the possession of a third party.

Assuming *arguendo* some information the government obtained through this search might, in other contexts, be available from third parties and not subject to a reasonable expectation of privacy, that was not the case here. Rather, here, the government directly searched private areas on the user's computer, without his

knowledge or consent. As one district court recognized:

> There is a significant difference between obtaining an IP address from *a third party* and obtaining it *directly from a defendant's computer*. . . If a defendant writes his IP address on a piece of paper and places it in a drawer in his home, there would be no question that law enforcement would need a warrant to access that piece of paper . . . Defendants nonetheless had a reasonable expectation of privacy in the locations where the IP addresses were stored, necessitating that law enforcement obtain a valid warrant before searching such locations.

United States v. Croghan, 209 F. Supp. 3d 1080, 1092-93 (S.D. Iowa 2016) (emphasis original).

3. The government's malware copied information from software operating on users' computers and sent the copied information to the FBI. That copying constitutes a Fourth Amendment seizure.

Again, a seizure occurs when the government meaningfully interferes with an individual's possessory interest in property. *Jacobsen,* 466 U.S. at 113. Courts recognize that individuals have possessory interests in information and that copying information interferes with that interest. *LeClair v. Hart*, 800 F.2d 692, 695, 696 n.5 (7th Cir. 1986) (recognizing it "is the information and not the paper and ink itself" that is actually seized); *see also United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1168-71 (9th Cir. 2010) (referring to copying of data as a "seizure").

The government apparently agrees on this point: the warrant itself described the copied information as the property "to be seized." Accordingly, when the

government's malware copied information from a user's computer, that copying constituted a Fourth Amendment seizure.

C. Other constitutionally suspect types of warrants offer far more particularity than the warrant here.

In light of the significant searches and seizures the warrant authorized, a specific, particularized warrant was critical. Yet even other types of warrants that stretch the Fourth Amendment's particularity requirement—like anticipatory warrants, "all persons" warrants, and roving wiretaps—provide greater particularity than the warrant used here, underscoring its unconstitutionality.

1. The warrant in this case was a species of constitutionally suspect warrant known as an "anticipatory warrant." An anticipatory warrant is based on "probable cause that at some future time (but not presently) certain evidence of a crime will be located at a specified place," 2 LaFave, *Search and Seizure* § 3.7(c), p. 398. Although not "categorically unconstitutional," warrants conditioned on a future event require an additional showing: the "likelihood that the condition will occur" and that the "object of seizure will be on the described premises." *United States v. Grubbs*, 547 U.S. 90, 94, 96 (2006). Were that not the case, "an anticipatory warrant could be issued for every house in the country, authorizing search and seizure *if* contraband should be delivered—though for any single location there is no likelihood that contraband will be delivered." *Id*. at 96 (emphasis in original).

The warrant here was unquestionably anticipatory. The search and seizure of an "activating computer" was predicated on a user logging into Playpen at some unspecified point in the future. *See* Warrant at 2.

However, the affidavit failed to describe, as *Grubbs* requires, the "likelihood that the condition w[ould] occur"—that a user would log into the website—for any specific user (or, for that matter, for any future registered user). The warrant thus more closely resembles the hypothetical warrant the Supreme Court cautioned against in *Grubbs*—a warrant for "every house in the country, authorizing search and seizure *if*" the predicate event occurs—than a particularized authorization to search a specific place or person.

Some courts have incorrectly found the warrant to be sufficiently particularized based on the observation that the "search applies only to computers of users accessing the website, a group that is necessarily actively attempting to access child pornography." *United States v. Anzalone*, 2016 WL 5339723 at *7 (D. Mass. Sep. 22, 2016). But this conclusion ignores the *Grubbs* Court's requirement that there be a connection—established and described *at the time the warrant is sought*—between the anticipated condition and a specific place to be searched. *Grubbs*, 547 U.S. at 96; *see also Carlson* R&R at 26 ("This Court is not aware of any case where a court has permitted the actual identification of the place to be searched to depend upon the occurrence of an anticipated event that has not yet

occurred.")

Indeed, no court would issue an analogous warrant in the physical world. For example, Philadelphia police undoubtedly have probable cause to believe the public sale of illegal drugs will occur in the city.[14] They can even point to specific events and locations—a concert at the Wells Fargo Center, for example—where sales are likely to occur. Yet no court would issue an anticipatory warrant that authorized the police to: (1) observe such public sales, (2) decide which suspects to pursue, and (3) subsequently (and surreptitiously) enter purchasers' homes in order to identify them.

Yet that is precisely what the warrant authorized here. The FBI was authorized to: (1) observe users as they attempted to access the website; (2) choose, at its discretion, which users to pursue; and (3) surreptitiously access those users' electronic devices.

An anticipatory warrant, like the one relied on here, would never issue in the physical world. There is no principled basis to allow one in the digital world.

2. "All persons" warrants are another unusual—and likewise constitutionally suspect—type of warrant that are nevertheless more particularized

[14] *Cf. Illinois v. Gates,* 462 U.S. 213, 238 (1983) (affidavit establishes probable cause to issue a search warrant if, "given all the circumstances, . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place.").

than the warrant here.

These warrants authorize the search of a particular place, as well as "all persons" on the premises when the search is conducted. *See Marks v. Clarke*, 102 F.3d 1012, 1029 (9th Cir. 1996). As a threshold matter, the constitutionality of these warrants is "far from settled law." *Mongham v. Soronen*, 2013 WL 705390, at *6 (S.D. Ala. Feb. 26, 2013); *see also Ybarra*, 444 U.S. at 92 n.4 ("Consequently, we need not consider situations where the warrant itself authorizes the search of unnamed persons in a place[.]"); *Doe v. Groody*, 361 F.3d 232, 243 (3d Cir. 2004) ("A search warrant for a premises does not constitute a license to search everyone inside."). Indeed, some courts have concluded that "all persons" warrants are *per se* unconstitutional. *See United States v. Guadarrama*, 128 F. Supp. 2d 1202, 1207 (E.D. Wis. 2001) (collecting cases and noting "the minority view" that "'all persons' warrants are facially unconstitutional because of their resemblance to general warrants.").

Even assuming their constitutionality as a general class, amici are not aware of an "all persons" warrant that comes close to approximating the reach of the warrant here. First, "all persons" warrants are by definition tied to the search of a particular physical location—something conspicuously absent here. Second, "all persons" warrants are necessarily limited by physical constraints. These warrants authorize searches of a small number of people physically present at a specific

location. *See State v. De Simone*, 288 A.2d 849, 853 (N.J. 1972) (collecting cases in which 10-30 individuals were searched). In contrast, here, the warrant authorized searches of over a hundred thousand users' devices in locations around the world. No comparable "all persons" warrant has ever issued. *See Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (noting electronic surveillance evades "ordinary checks" on abuse, including limited police resources)

3. Finally, warrants for roving wiretaps—yet another species of suspect warrant—permit interception of a *particular, identified* suspect's communications, even where the government cannot identify in advance the particular facilities that the suspect will use. *See, e.g., United States v. Petti*, 973 F.2d 1441, 1444-46 (9th Cir. 1992); *United States v. Jackson*, 207 F.3d 910, 914 (7th Cir. 2000), *vacated on other grounds by* 531 U.S. 953 (2000) (citing cases).[15] In a departure from usual Fourth Amendment practice, roving wiretaps do not describe the "place to be searched" with absolute particularity; instead, the place to be searched is tied to the identification of a particular, named suspect, and is then coupled with additional safeguards mandated by federal statute. 18 U.S.C. § 2518(11); *see also United States v. Silberman*, 732 F. Supp. 1057, 1060 (S.D. Cal. 1990), *aff'd sub nom.*

[15] In an application for a fixed wiretap on a particular facility, "the anticipated speaker need be identified only if known." *Petti*, 973 F.2d at 1445 n.3. Nevertheless, courts require stringent minimization of the conversations captured. *See Berger v. New York*, 388 U.S. 41, 56, 59 (1967).

United States v. Petti, 973 F.2d 1441.[16]

Here, by contrast, no specific suspect or user was named in the warrant, though the government could have done so. Instead, the government sought authorization to search *anyone* accessing the site. Nor is this a case where Congress has established a specific surveillance framework imposing additional safeguards in the face of constitutional uncertainty. Instead, the government made up rules—broad ones—as it went along.

* * *

In sum, roving wiretaps authorize surveillance of *specific* people using unnamed facilities. "All persons" warrants authorize the search of unnamed people in *specific* places. And anticipatory warrants authorize searches based upon the likelihood of a particular future event occurring. But no constitutionally valid warrant can authorize the search of unnamed (and unlimited) persons in unnamed (and unlimited) places based upon the unsupported likelihood of a future event. Yet that is precisely what the warrant did here.

II. HACKING INTO A COMPUTER IS NOT THE INSTALLATION OF A TRACKING DEVICE UNDER RULE 41(b)(4).

The warrant was invalid for an additional reason: hacking into a computer to obtain identifying information does not constitute the installation of a device which

[16] Courts have determined that the "conditions imposed on 'roving' wiretap surveillance by [these safeguards] satisfy the purposes of the particularity requirement." *Petti*, 973 F.2d at 1445.

permits the tracking of "the movement of a person or property." Fed. R. Crim. P. 41(b)(4).

The government has urged courts to adopt a "flexible" approach to Rule 41. *Werdene*, 188 F. Supp. 3d at 441. Under the government's view, an installation under subsection (b)(4) need not occur in the district where the search or seizure was to occur; rather, the installation could be carried out anywhere. *Levin,* 186 F. Supp. 3d at 34. Indeed, the government's interpretation would not even require that a "tracking device" be used to "track the movement" of a person or property at all; *Carlson* R&R at 12; rather, a warrant under Rule 41(b)(4) could authorize remote installation of any number of electronic monitoring devices—devices to monitor electricity usage or health information, for example.

In reality, the "flexible" reading urged by the government requires outright revision to the terms of Rule 41(b)(4). The Rule was, in fact, subsequently revised to allow a magistrate to issue an out-of-district warrant for "remote access" to a computer if its location "has been concealed through technological means." Fed. R. Crim. P. 41(b)(6) (Dec. 1, 2016). However, this change was made after the search here, further evidence that the warrant was not authorized under Rule 41 as it then stood.

The use of malware in this case fails to comport with Rule 41(b)(4) in

multiple respects, as the majority of district courts to consider the issue[17]—correctly concluded.

A. The government's malware was not used to "track the movement" of a person or property.

First and most fundamentally, the government's malware was not installed "to track the movement" of anything—including data, Appellant's computer, or Appellant himself.

Rule 41(b)(4) allows a magistrate to issue a warrant to install "a tracking device," which may be used "to track the movement of a person or property located within the district, outside the district, or both." However, the government's malware was never designed to "track" anything—let alone track location. Instead, as the warrant application states, the purpose of the malware was to obtain "environmental variables and certain registry-type information," including the computer's actual IP address, the type of operating system the computer was running, and computer "host name," among other information.

---

[17] Amici are aware of only a few courts that have concluded the warrant was valid under Rule 41. *See, e.g.*, *United States v. Johnson,* 2016 WL 6136586 (W.D. Mo. Oct. 20, 2016); *United States v. Dzwonczyk*, No. 15-CR-3134 (D. Neb. Oct. 5, 2016) (magistrate's report and recommendation); *United States v. Smith*, No. 15-CR-467 (S.D. Tex. Sept. 28, 2016). Of those, three arose in the Eastern District of Virginia, where the magistrate judge who issued the warrant was located. *See, e.g.*, *United States v. Darby*, 190 F. Supp. 3d 520 (E.D. Va. 2016).

Instead, the majority of courts have determined that Rule 41 was violated but have reached different conclusions concerning suppression. *Compare Tippens* Order at 13-16, *with Croghan*, 209 F. Supp. 3d at 1092-93.

Warrant Aff., ¶ 34.

Although the seized information may ultimately have assisted the FBI in identifying a particular user, on its own the seized information says precious little about location. In fact, in many instances, the information may not have revealed *anything* about a user's location. For example, IP addresses alone may tell the FBI information about an individual's general location (akin to a telephone area code). But they also might not reveal any accurate or reliable information about location.[18] In this investigation, it was generally only after the FBI took additional investigative steps that any reliable location information was obtained.

In sum, the malware "did not 'track' the 'movement of a person or object.' Indeed, it did not 'track' the 'movement' of anything." *Croghan*, 209 F. Supp. 3d at 1088.

B. The government's malware was "installed" where the target computers were located.

Second, the government's malware was not "installed" in the Eastern District of Virginia—neither in a technical nor legal sense.

Rule 41(b)(4) requires that the tracking device be "install[ed] within the district." Technically speaking, "installation" of the malware—if it occurred

[18] *See Unreliable Informants: IP Addresses, Digital Tips and Police Raids*, EFF (Sept. 2016), https://www.eff.org/files/2016/09/22/2016.09.20_final_formatted_ip_address_white_paper.pdf.

anywhere—occurred only when the NIT executed the exploit that allowed the FBI to place code on the target computer. That occurred on a targeted computer, not on the server that delivered the NIT code.[19] Legally, the relevant installation "event," for purposes of the Fourth Amendment and Rule 41, occurs when the government's code seizes control of the software running on a user's device. *See* Section I.B.1, *supra*.

Even if the government contends users made "a virtual trip" via the Internet to Virginia, that purported "trip" resulted in nothing more than a request to send information to a device in Pennsylvania. *See* Warrant Aff., ¶ 33. And it was not until that information—including the government's malware—reached Pennsylvania that it had its intended effect.

Just as a GPS device is installed when it is affixed to a suspect's car, *see Jones*, 565 U.S. at 411, government malware is installed—to the extent it is installed anywhere—when the malware alters code on and seizes control of a user's device.

[19] Installation "typically involves code being copied/generated from the installation files to new files on the local computer for easier access by the operating system." *Installation (computer programs)*, Wikipedia, https://en.wikipedia.org/wiki/Installation_(computer_programs) (last visited April 24, 2017).

CONCLUSION

For the reasons described above, the warrant violated the Fourth Amendment and Rule 41 of the Federal Rules of Criminal Procedure.

Dated: April 26, 2017

By: /s/ Andrew Crocker
Andrew Crocker
Counsel for Amici Curiae
Mark Rumold
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
andrew@eff.org

/s/ Witold J. Walczak
Witold J. Walczak
AMERICAN CIVIL LIBERTIES UNION OF PENNSYLVANIA
247 Fort Pitt Blvd.
Pittsburgh, PA 15222
Telephone: (412) 681-7736
Fax: (412) 681-8707
VWalczak@aclupa.org

COMBINED CERTIFICATIONS

I hereby certify as follows:

1. That I, Andrew Crocker, counsel for *Amici Curiae*, am a member of the Bar of this Court.

2. That the foregoing brief of *Amici Curiae* complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B). The brief is printed in proportionally spaced 14-point Times New Roman font, using Microsoft® Word for Mac 2011 and there are 6,492 words in the brief according to the word count of the word-processing system used to prepare the brief (excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii)). The brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5), and with the type style requirements of Fed. R. App. P. 32(a)(6).

3. That I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Third Circuit, pursuant to Third Circuit Rule 25.1(b) by using the appellate CM/ECF system on April 26, 2017. All participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

4. That the text of the electronic brief is identical to the text of the seven paper copies mailed to the Court pursuant to Local Rule 31.1(b)(3).

5. That the electronic file of this brief was scanned with Avast antivirus

software version 11.7.45814 and that no virus was detected.

Dated: April 26, 2017

By: /s/ Andrew Crocker
Andrew Crocker

Counsel for Amici Curiae Electronic Frontier Foundation and American Civil Liberties Union of Pennsylvania