NO. 16-3976, 16-3982

IN THE UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT

UNITED STATES OF AMERICA,

PLAINTIFF-APPELLANT,

V.

STEVEN SHANE HORTON,

BEAU BRANDON CROGHAN

DEFENDANTS-APPELLEES.

On Appeal from the United States District Court
For the Southern District of Iowa – Council Bluffs
Case No. 15-cr-00051

The Honorable Robert W. Pratt, United States District Court Judge

BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANTS-APPELLEES AND AFFIRMANCE

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

Counsel for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, amicus curiae Electronic Frontier Foundation states that it does not have a parent corporation and that no publicly held corporation owns 10% or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

Constitutional Provisions

STATEMENT OF INTEREST[1]

Amicus curiae the 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 for 25 years. With roughly 33,000 active donors, EFF represents the interests of technology users in court cases and broader policy debates surrounding the application of law in the digital age.

EFF regularly participates as amicus in cases addressing constitutional rights—and, in particular, the Fourth Amendment—and their relationship to new law enforcement surveillance techniques. *See, e.g.*, *Riley v. California*, 134 S. Ct. 2473 (2014); *Maryland v. King*, 133 S. Ct. 1958 (2013); *United States v. Jones*, 132 S. Ct. 945 (2012).

Additionally, EFF participated as amicus at the district court level in two cases arising from the same investigation at issue here. *See United States v. Matish*, No. 16-cr-0016 (E.D. Va.) (ECF No. 42-2); *United States v. Owens*, 16-cr-0038 (E.D. Wisc.) (ECF No. 42-1).

[1] Pursuant to Federal Rule of Appellate Procedure Rule 29(c), amicus certifies that no person or entity, other than amicus, 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. Pursuant to Federal Rule of Appellate Procedure Rule 29(a)(2), amicus represents that all parties have consented to the filing of this brief.

INTRODUCTION

This appeal—among the first of its kind—centers on a relatively new law enforcement surveillance technique: "hacking" the electronic devices of citizens. More fundamentally, this case concerns the appropriate 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 hundreds, if not thousands, of times.

And *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 hundreds or thousands of homes, without identifying specific buildings or specifying where those buildings were located, 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 ran afoul of the Fourth Amendment's requirements, which "reflect 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.

Additionally, the warrant failed to satisfy the basic procedural safeguards required by the now-amended Rule 41 of the Federal Rules of Criminal Procedure. The government's malware was not a "tracking device," and it was not installed in the Eastern District of Virginia. Thus, the magistrate who issued the warrant lacked authority to do so, as the district court correctly concluded.

Under either analysis, the warrant was invalid.

FACTUAL BACKGROUND

This case, and hundreds of others like it across the country, stems from the FBI's investigation of "Playpen," a website hosting child pornography. The FBI investigation involved hacking into an unknown number of computers using government-developed malware in order to bypass Tor, a software program used for online anonymity.

Operating on a tip from a foreign government, the FBI obtained a warrant and seized the servers that hosted Playpen in January 2015. *See* Warrant Aff., ¶ 28.[2] Once in physical possession of the servers, the FBI assumed the role of website administrator. *Id*., ¶30. During that time, the government 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 a privacy-enhancing technology known as "Tor."

Tor (short for "The Onion Router") was developed to allow users to circumvent restrictions on speech and to evade pervasive Internet surveillance. Tor is used by journalists, human rights advocates, lawyers, and governments—including the federal government.[3]

Tor consists of a computer network and software that work together to

---

[2] The warrant at issue in this case, its two incorporated attachments, and the warrant application submitted by FBI Special Agent Douglas Macfarlane, were filed as Exhibit A to Mr. Croghan's motion to suppress (DCD No. 33). References herein to the "Warrant," "Warrant Attach." or the "Warrant Aff." are to those documents.

[3] 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.en. Recognizing the privacy-enhancing value of the technology, amicus 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*.

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, to avoid tracking of their browsing behaviors, and to facilitate other forms of anonymous communication.[4]

The Tor network consists of volunteer-operated computers, known as "nodes" or "relays," which make it possible for Tor users to connect to websites "through a series of virtual tunnels rather than making a direct connection."[5] 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 location of the site.[6] Other Tor users can connect to these hidden services, without knowing the actual address of the site and without the site knowing information about visitors that would ordinarily be disclosed in the course of web browsing, including the public Internet Protocol (IP) address assigned to them by their Internet Service Provider (ISP).

Playpen operated as a Tor hidden service. Warrant Aff., ¶ 12.

---

[4] *Id*.

[5] *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.

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

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 who logged into the site. *See* District Court Order on Motions to Suppress ("Suppression Order") at 3. 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.[7]

The government developed the malware in this case, and it invented the term "Network Investigative Technique" or "NIT" to describe it. As a technical matter, there is little difference between a NIT and the types of malware used by identity thieves or other criminal "hackers."[8]

---

[7] *See* Robert Moir, *Defining Malware: FAQ*, Microsoft TechNet (Oct. 2003), https://technet.microsoft.com/en-us/library/dd632948.aspx.

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

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. 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.[9]

Here, it appears that the government employed at least two different delivery methods for its malware for different users of the site. Warrant Aff., ¶ 32 n.8. But the operation of the malware was similar, regardless of its method of delivery: computer code served by the government to the target computers used one or more vulnerabilities in the 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.[10]

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

---

us/library/dd632947.aspx.

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

[10] *See 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.

ARGUMENT

The warrant in this case did not approach the "scrupulous exactitude" to the Fourth Amendment that the surveillance technique requires. *Stanford*, 379 U.S. at 485.

On its face, 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. Those facts, alone, are sufficient to render the warrant invalid.

The breadth of the warrant is underscored by the significance of the

activities it authorized: surreptitiously infecting an individual's software and computer with malware, searching the computer, and then copying data from that computer. Individually, each of these activities is a significant Fourth Amendment event; collectively, more significant; and repeated hundreds, if not thousands of times, more significant still.

Ultimately, the warrant is invalid because it lacks the careful tailoring and particularity the Fourth Amendment requires. Even when compared to other types of constitutionally-suspect warrants, the warrant here represents a serious departure from traditional Fourth Amendment jurisprudence, more closely approximating the general warrants and writs of assistance the Fourth Amendment was designed to prevent.

Moreover, as the district court and, indeed, the majority of district courts to consider the issue, correctly held: the warrant also violated Rule 41 of the Federal Rules of Criminal Procedure because it authorized searches in unknown places outside of the issuing magistrate's district. The ruling was correct, and there is no reason to disturb it.

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 the "issu[ance] of warrants on loose" or "vague" bases. Wayne R. LaFave, *Search and Seizure* § 4.6(a) (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." *Massachusetts v. Sheppard*, 468 U.S. 981, 988 n.5 (1984).

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. 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; *Marron v. United States,* 275 U.S. 192, 195 (1927). Each person or place to be searched requires a specific description in the warrant, accompanied by an individualized showing of probable cause. *United States v. Alberts*, 721 F.2d 636, 639 (8th Cir. 1983); *United States v. Sims*, 553 F.3d 580, 582 (7th Cir. 2009). For example, a warrant to arrest a specific individual is not sufficiently particularized to give officers the "authority to enter the homes of third parties" to search for the individual because it "specifies only the object of a search" and "leaves to the unfettered discretion of the police the decision as to which particular homes should be searched." *Steagald v. United States*, 451 U.S. 204, 220 (1981); *see also Walter v. United States*, 447 U.S. 649, 656-57 (1980) ("[A] warrant to search for a stolen refrigerator would not authorize the opening of desk drawers.").

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

Compounding matters, the warrant failed to provide any specificity about the

place to be searched—the location of "activating computers."[11] *See* Warrant Attach. A. Instead, the warrant authorized the search of "any" activating computer, no matter where that computer might be located. Because an activating computer could be located anywhere in the world, the warrant potentially authorized FBI searches and seizures in every U.S. state, every U.S. territory, and every country around the world.[12]

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

2. The absence of particularity was not compelled by the technology at issue.

The particularity requirement is context-dependent, and the specificity required in a warrant will vary based on the amount of information available and the scope of the search to be executed. *United States v. Horn*, 187 F.3d 781,788 (8th Cir. 1999); *United States v. Mousli*, 511 F.3d 7, 13 (1st Cir. 2007) (upholding

[11] The warrant listed the Eastern District of Virginia as the location of the property to be searched. *See* Warrant. That was incorrect: the searches occurred on users' computers, wherever they were located.

[12] Indeed, it appears that the government did conduct overseas searches based on the warrant. Joseph Cox, *New Case Suggests the FBI Shared Data from Its Mass Hacking Campaign with the UK*, Motherboard (Feb. 10, 2016), https://motherboard.vice.com/read/new-case-suggests-the-fbi-shared-data-from-its-mass-hacking-campaign-with-the-uk. The government's decision to conduct these searches—and the magistrate's decision to authorize them—raises special considerations when the searches occur worldwide. *See Microsoft Corp. v. United States*, 829 F.3d 197, 212 (2d Cir. 2016) (noting that Fourth Amendment traditionally limits warrants to domestic investigations).

particularity of warrant where "police used all of the information reasonably available to them to secure as particularized a warrant as possible."). As the Fifth Circuit has explained, "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) (emphasis added). "[C]ourts have therefore demanded that . . . the warrant description must be as particular as circumstances permit." *United States v. Jones*, 54 F.3d 1285, 1291 (7th Cir. 1995) (internal quotations and citations omitted).

The government relied on a generic classification—"activating computers"—that potentially encompassed any of the site's 150,000 registered accounts; far more precision was not only possible but necessary. The FBI possessed the server that hosted the site and had a clear window into user activity. Based on this activity, the government could track: (1) which users were posting and accessing specific information; (2) the frequency with which those users were doing so; and (3) the nature of the information they posted or accessed. Law enforcement could have done more still—such as reviewing site activity for evidence of a user's location or actual identity.

The inclusion of this information in the warrant application would have allowed the government to obtain a warrant based on *specific* facts, tied to *specific* users, thus authorizing searches and seizures against those specific, named users

and their specific computers.

Although the actual physical location of these specific users might still be unknown, the warrant could and should have targeted specific individuals based on specific probable cause determinations. It is by no means "immaterial" that the government could have narrowed the scope of the Playpen warrant. *United States v. Matish*, 2016 WL 3545776, at *14 (E.D. Va. 2016). Here, "circumstances permit[ted]" the government to submit more particular information; it was thus required to do so. *Jones*, 54 F.3d at 1291.

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. Accordingly, particularity was crucial, given the significant Fourth Amendment events that occurred each of the hundreds or thousands of times the government deployed its malware.

Each use of the NIT triggered three Fourth Amendment events: (1) an entry into and seizure of the user's computer; (2) a search of the private areas of that computer; and (3) a seizure of private information from the computer.

Critically, the warrant was not limited to a single search or seizure; nor was it limited to all three for a specific user. Rather, on its face, the warrant authorized

the FBI to repeatedly execute these searches and seizures—upwards of hundreds of thousands of times.

1. The government's malware exploited an otherwise unknown or obscure software vulnerability, 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 "interfere[d]" 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" over the software running on a user's computer, even if limited, constitutes a seizure. *See Jacobsen,* 466 U.S. at 120-21 & n.18; *see* Report and Recommendation at 11-12, *United States v. Arterbury*, 15-cr-0018 (N.D. Ok. filed Apr. 25, 2016) (ECF No. 42); *cf. Jones*, 132 S. Ct. at 949 (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*, 134 S. Ct. 2473 (2014), 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)). It is no surprise, then, that courts uniformly recognize the need for warrants prior to searching computers. *See, e.g.*, *United States v. Wurie*, 728 F.3d 1, 8-10 (1st Cir. 2013) (warrant required for search of phones and computers), *aff'd sub nom. Riley v. California*, 134 S. Ct. 2473 (2014); *United States v. Payton*, 573 F.3d 859, 862 (9th Cir. 2009); *United States v. Andrus*, 483 F.3d 711, 718 (10th Cir. 2007), *reh'g denied*, 499 F.3d 1162 (10th Cir. 2007);.

In this case, a search occurred because the government's malware operated directly on users' computers—a private area subject to a user's reasonable

expectation of privacy. *United States v. Stults*, 575 F.3d 834, 843 (8th Cir. 2009) (recognizing that, as a "general matter," individuals have a reasonable expectation of privacy in personal computer). 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).

Some district courts considering these cases have incorrectly reasoned that no search occurred because individuals have no reasonable expectation of privacy in IP addresses. *See, e.g.*, *United States v. Werdene*, No. 15-CR-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016) (ECF No. 33). Those decisions rely on *Smith v. Maryland*, 442 U.S. 735 (1979), and its related progeny, which involved warrantless access to information possessed *by a third party*. While some information the government obtained through this search might, in other contexts, be available from third parties, that was not the case here. Rather, here, the government directly searched private areas on the user's computer without their knowledge or consent. As the district court correctly 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 . . . While the IP addresses may have themselves been evidence of a crime, Defendants nonetheless had a reasonable expectation of privacy in the locations where the IP addresses were stored[.]

Suppression Order at 18 (emphasis in original).

Thus, the relevant question in this case is not whether the defendant had a reasonable expectation of privacy *in the information* obtained through the search, but whether the defendant had a reasonable expectation of privacy *in the place where the search occurred*. *See Rakas*, 439 U.S. at 143; *Riley*, 134 S. Ct. at 2488. A search that occurs inside a person's home, on their personal computer, must be provided the Fourth Amendment's highest protection.

3. The government's malware copied information from software operating on users' computers and sent the copied information to the FBI. That copying constituted 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). This is so because "the Fourth Amendment protects an individual's possessory interest in information itself, and not simply in the medium in which it exists." *United States v. Jefferson*, 571 F. Supp. 2d 696, 702 (E.D. Va. 2008); *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1168-71 (9th Cir. 2010) (referring to copying of data as a "seizure");

Microsoft Corp., 829 F.3d at 219-220 (same).

On this point, the Government is in apparent agreement: 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 series of significant searches and seizures the warrant authorized, particularity was critical. Yet even other types of warrants that stretch the Fourth Amendment's particularity requirement—like anticipatory warrants, roving wiretaps, and "all persons" warrants—provide greater particularity than the warrant used here, underscoring its unconstitutionality.

1. The warrant here was a species of constitutionally-suspect warrant known as an "anticipatory warrant." An anticipatory warrant is one 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 (4th ed. 2004). Although they are 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 an anticipatory one. 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 single 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*, No. 15-CR-10347, 2016 WL 5339723 at *7 (D. Mass. Sep. 22, 2016). But this runs afoul of the *Grubbs* Court's admonition that there must 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.

Indeed, no court would issue an analogous warrant for similar conduct in the physical world. For example, police in Iowa undoubtedly have probable cause to believe that the public sale of illegal drugs will occur in the state. They can even point to specific public events and locations—the Iowa State Fair, for example—where these sales are likely to occur. Yet no court would issue a warrant that authorized police to: (1) observe such public sales, (2) decide which suspects to pursue, and (3) subsequently (and surreptitiously) enter the homes of those purchasers 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 their own discretion, which users to pursue; and (3) surreptitiously access electronic devices—containing the very "privacies of life," *Riley*, 134 S. Ct. at 2495—of those users.

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

These warrants authorize the search of a particular place, as well as "all persons" on the premises at the time 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 v. Illinois*, 444 U.S. 85, 92 n.4 (1979) ("Consequently, we need not consider situations where the warrant itself authorizes the search of unnamed persons in a place[.]"). 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, held or suggested by eight jurisdictions, is that 'all persons' warrants are facially unconstitutional because of their resemblance to general warrants.").

Even assuming their constitutionality as a general class, amicus is not aware of an "all persons" warrant that comes close to approximating the scope and reach of the warrant at issue 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 generally authorize search of a small number of people physically present at a specific location. *See State v. De Simone*, 60 N.J. 319, 327 (N.J. 1972) (collecting cases in which 10-25 individuals were searched). In contrast, the warrant here, in principle, authorized searches of over a hundred thousand users' devices around the world. And even in practice, the searches carried out under the auspices of the warrant were vast—encompassing hundreds or even thousands of

computers. No comparable "all persons" warrant has ever issued. *See Jones*, 132 S. Ct. at 956 (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).[13] 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. United States v. Petti*, 973 F.2d 1441 (9th Cir. 1992).[14]

Here, by contrast, no specific suspect—or user—was named in the warrant.

---

[13] 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 on a wiretap. *See Berger v. New York*, 388 U.S. 41, 56, 59 (1967).

[14] 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.

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

Rule 41(b)(4) allows a magistrate judge "to issue a warrant to install within the district 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." *Id.*

The government urges this Court to adopt a "flexible" approach to Rule 41.

Appellant's Br. at 24. But the "flexible" reading urged by the government requires an outright revision to the terms of Rule 41 (b)(4).

Under the government's view, an installation need not occur in the district where the search or seizure was to occur; rather, the installation could be carried out anywhere in the country. Indeed, the government's interpretation would not even require that a "tracking device" be used to "track the movement" of an individual or property at all; rather, a warrant under Rule 41(b)(4) could authorize the installation of any number of electronic monitoring devices remotely—devices to monitor electricity usage or health information, for example.

The use of malware in this case fails to comport with Rule 41(b)(4) in multiple respects, as the district court below—and the majority of district courts to consider the issue[15]—correctly concluded.

[15] Amicus is aware of only seven 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 seven, three cases arose in the Eastern District of Virginia—the district where the magistrate judge that issued the warrant was located. *See, e.g.*, *United States v. Darby*, 2016 WL 3189703 (E.D. Va. June 3, 2016).

In contrast, the majority of courts have determined that Rule 41 was violated but have reached different conclusions concerning suppression. *See, e.g.*, *Werdene*, 2016 WL 3002376, *7; *United States v. Levin*, 186 F.Supp. 3d. 26 (D. Mass. 2016).

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, the appellees' computers, or appellees themselves.

As the warrant application states, the deployment of the government's malware was designed 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. 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 a user's *location*. Indeed, in many instances, the information seized 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 information about location.[16] In this investigation, it was generally only after the FBI took additional investigative steps that any reliable information related to location was

[16] IP addresses are at best only a modest proxy for location; at worst, they provide no useful information about an individual's location. *See Unreliable Informants: IP Addresses, Digital Tips and Police Raids*, EFF (Sep. 2016), https://www.eff.org/files/2016/09/22/2016.09.20_final_formatted_ip_address_white_paper.pdf.

actually obtained.

As the district court correctly identified, the malware at issue here "did not 'track' the 'movement of a person or object.' Indeed, it did not 'track' the 'movement' of anything." Suppression Order at 10.

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.

Technically speaking, "installation" of the malware occurred—if it occurred anywhere—only when the NIT executed the exploit that allowed the FBI to place code on the target computer. That execution occurred on a targeted computer, *not* on the server that delivered the NIT code.[17]

Legally, and as described previously, 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 supra* Section I.B.1.

Even if, as the government has contended, appellees made a "virtual trip via the Internet to Virginia," Appellant Br. at 23, that alleged "trip" resulted in nothing

[17] 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).

more than a request to send information to their device in Iowa. *See* Warrant Aff., ¶ 33. And it was not until that information—including the government's malware—reached Iowa that it had its intended effect.

Just as a GPS device is installed when it is affixed to a suspect's car, *see Jones*, 132 S. Ct at 948, government malware is installed—to the extent it is "installed" anywhere—when the malware alters code on a user's device and seizes control of that device. *See supra* Section I.B.1.

CONCLUSION

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

Dated: January 6, 2017

By: /s/ Mark Rumold
Mark Rumold
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
mark@eff.org

Counsel for Amicus Curiae Electronic Frontier Foundation

CERTIFICATE OF COMPLIANCE WITH RULE 32(A)

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because:

[X] this brief contains [6,339] words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii), or

[ ] this brief uses a monospaced typeface and contains [less than 650] lines of text, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii)

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5), and the type style requirements of Fed. R. App. P. 32(a)(6) because:

[X] this brief has been prepared in a proportionally spaced typeface using [Microsoft Word 2010] in [14 point Times New Roman font], or

[ ] this brief has been prepared in a monospaced typeface using [name and version of word processing program] with [number of characters per inch and name of type style].

Dated: January 6, 2017

By: /s/ Mark Rumold
Mark Rumold

Counsel for Amicus Curiae
Electronic Frontier Foundation

CERTIFICATE OF COMPLIANCE
WITH EIGHTH CIRCUIT RULE 28A(h)

Pursuant to this Court's Rule 28A(h), I hereby certify that the electronic version of this Brief of Amicus Curiae Electronic Frontier Foundation has been scanned for viruses and is virus-free.

Dated: January 6, 2017

By: /s/ Mark Rumold
Mark Rumold

Counsel for Amicus Curiae
Electronic Frontier Foundation

CERTIFICATE OF SERVICE

I hereby certify that on January 6, 2017, I electronically filed the foregoing brief with the Clerk of the Court for the United States Court of Appeals for the Eighth Circuit by using the CM/ECF system. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system, pursuant to Eighth Circuit Rule 25A.

Dated: January 6, 2017

By: /s/ Mark Rumold
Mark Rumold

Counsel for Amicus Curiae
Electronic Frontier Foundation