NO. 16-1401

IN THE UNITED STATES COURT OF APPEALS
FOR THE TENTH CIRCUIT

UNITED STATES OF AMERICA,

PLAINTIFF-APPELLANT,

v.

ANDREW JOSEPH WORKMAN

DEFENDANT-APPELLEE.

On Appeal from the United States District Court
for the District of Colorado, Denver
No. 15-cr-0397-RBJ

The Honorable R. Brooke Jackson, United States District Court Judge

BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT-APPELLEE 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 Federal Rules of Appellate Procedure 26.1 and 29(a)(4)(A), amicus curiae states that it does not have a parent corporation and that no publicly held corporation owns 10% or more of its stock.

Pursuant to Federal Rule of Appellate Procedure Rule 29(a)(4)(E), amicus curiae certifies that no person or entity, other than amicus, its members, or its 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

Constitutional Provisions

Statutes

Rules

Other Authorities

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 for 26 years. With roughly 37,000 active donors, EFF represents technology users' interests in court cases and broader policy debates. EFF regularly participates as amicus in cases addressing the Fourth Amendment and its relationship to technology and new surveillance techniques.

Relevant here, EFF has participated as amicus in other cases arising from the same investigation at issue in this case, including cases before the First and Eighth Circuits, and in two cases at the district court level. *See United States v. Levin*, 16-1567 (1st Cir.); *United States v. Croghan*, Nos. 16-3976, 16-3982 (8th Cir.); *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 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" citizens' electronic devices. More fundamentally, the 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 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 thousands homes, in states across the country, without identifying any specific home or specifying where those homes 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); *see also O'Rourke v. City of Norman*, 875 F.2d 1465, 1472-1473 (10th Cir. 1989).

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 procedural 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, and as the district court correctly concluded, 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]

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, 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—

---

[2] *See Order on Defendants' Motion to Dismiss Indictment, Defendants' Motion to Suppress Evidence, Defendants' Motion to Exclude Evidence, and Third Order on Defendants' Motion to Compel Discovery* [hereafter, "*Tippens* Order"] at 5, *United States v. Tippens*, et al., Case No. 16-05110-RJB (W.D. Wash. Nov. 30, 2016) (ECF No. 106) (JA.347).

[3] 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 an Addendum to the Government's Brief. *See* Addendum, A20-58. References herein to the "Warrant," "Warrant Attach." or the "Warrant Aff." are to those documents, respectively.

including the federal government.[4]

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, to avoid tracking of their browsing behaviors, and to facilitate other forms of anonymous communication.[5]

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."[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

---

[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, 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*.

[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.

to these hidden services, without knowing the actual address of the site 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 a user by their Internet Service Provider (ISP).

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 who logged 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]

[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,

The government developed the malware in this case and coined 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."[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 the users' software to surreptitiously deliver and install the NIT.

---

integrity, or availability of the victim's data, applications, or operating system." Murugiah Souppaya and Karen Scarfone, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, NAT'L INST. OF STANDARDS AND TECH. SPECIAL PUBLICATION (July 2013), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

[9] 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-us/library/dd632947.aspx.

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

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 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]

---

[11] *See supra* n. 8.

[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,

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, 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

---

2016, https://motherboard.vice.com/read/fbi-hacked-over-8000-computers-in-120-countries-based-on-one-warrant.

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); *see also United States v. Leary*, 846 F.2d 592, 600-606 (10th Cir. 1988) (analyzing warrant that was "overbroad in every respect").

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 over 8,000 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; *Leary*, 846 F.2d at 600. Each person or place to be searched requires a specific description in the warrant, accompanied by an individualized showing of probable cause. *Id*. at 605; *see also Steagald v. United States*, 451 U.S. 204, 220 (1981) (noting that 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). Ultimately, particularity ensures that searches are "confined in scope." *Voss v. Bergsgaard*, 774 F.2d 402, 404 (10th Cir. 1985).

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

The warrant here did not identify any particular person or thing 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. *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."[13] *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, the warrant, on its face, authorized FBI searches and seizures in every U.S. state, every territory, and every country around the world.[14]

2. The absence of particularity was not compelled by the technology at issue. Although 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, the warrant application must provide "as much specificity as the government's knowledge and circumstances allow." *Cassady v. Goering*, 567 F.3d 628, 635 (10th Cir. 2009) (internal quotations and citations omitted). 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. *Id*.

---

[13] 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.

[14] As previously noted, this was not merely hypothetical. The government conducted searches in over 100 countries based on the warrant. *See Tippens* Order at 5.

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).

Although warrants may describe items in broad or generic terms, the description must nevertheless be "as specific as the circumstances permit." *Leary,* 846 F.2d 592, 600 (10th Cir. 1988); *cf. United States v. Bright*, 630 F.2d 804, 812 (5th Cir. 1980) ("[G]eneric classifications in a warrant are acceptable only when a more precise description is not possible.")

Here, *far* more precision was possible.

The FBI possessed the server that hosted the site and, thus, had a clear window into user activity on it. 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.

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.

Law enforcement could have done more still—such as reviewing site activity for evidence of a user's actual location or identity. 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's breadth.

"Yet the government chose to include none of these limiting factors." *Leary*,

846 F.2d at 604. Instead, the government 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 warrant application, thereby narrowing the scope of the warrant. *United States v. Matish*, 2016 WL 3545776, at *14 (E.D. Va. 2016). Nor is this empty formalism. 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. A specific and particularized warrant was thus crucial, given the significant Fourth Amendment events that occurred each of the thousands of times the government deployed its malware.

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.

Critically, the warrant was not limited to a single search or seizure; nor was it limited to an entry, search, and seizure for a specific 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 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. 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*, 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)). 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. Andrus*, 483 F.3d 711, 718 (10th Cir. 2007), *reh'g denied*, 499 F.3d 1162 (10th Cir. 2007); *accord United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004); *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' personal 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, some district courts have improperly focused on the *information obtained* from the search rather than *the place where the search occurred*. Those courts then incorrectly conclude that no Fourth Amendment search occurred because individuals have no reasonable expectation of privacy in IP addresses. *See, e.g.*, *United States v. Werdene*, 2016 WL 3002376 (E.D. Pa. May 18, 2016). Those decisions rely on *Smith v. Maryland*, 442 U.S. 735 (1979), and its related progeny, which involved warrantless access to information in the possession of a third party.

Assuming *arguendo* that some information the government obtained through this search might, in other contexts, be available from third parties and not subject

to a reasonable expectation privacy, 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 one 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[.]

United States v. Croghan, 2016 WL 4992105, at *7 (S.D. Iowa Sep. 19, 2016) (emphasis in 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").

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, 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 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. 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*, 2016 WL 5339723 at *7 (D. Mass. Sep. 22, 2016). But this conclusion ignores the *Grubbs* Court's requirement: 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, Denver police undoubtedly have probable cause to believe the public sale of illegal drugs will occur in the city.[15] They can even point to specific events and locations—a concert at Red Rocks Amphitheatre, for example—where these sales are likely to occur. Yet no court would issue a warrant that authorized the 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 discretion, which users to pursue; and (3) surreptitiously access the electronic devices of those users.

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 than the warrant issued here.

---

[15] *Cf. Illinois v. Gates,* 462 U.S. 213, 238 (1983) (holding that an 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.").

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 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 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 generally authorize searches 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, 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).[16] 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.[17]

---

[16] 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).

[17] 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.

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

The government urges this Court to adopt a "flexible" approach to Rule 41. Gov. Br. at 22. 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. 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.

In reality, the "flexible" reading urged by the government requires an 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 provision was not available at the time of the search here, further evidence that the warrant was not authorized under Rule 41 as it then stood. *See* A.008.

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[18]—correctly concluded.

[18] Amicus is aware of only a handful of 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

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, appellee's computer, or appellee 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." *Id.* 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. 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

---

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).

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*, 2016 WL 4992105, *7-8.

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.[19] In this investigation, it was generally only after the FBI took additional investigative steps that any reliable location-information was obtained.

In sum, and as the district court correctly recognized, the malware at issue here did not "track[] the data as it moved through various relay nodes." A.008. Indeed, it did not track anything at all.

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 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.[20] Legally, the relevant installation "event,"

---

[19] 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.

[20] Installation "typically involves code being copied/generated from the

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, as the government contends, appellee made "a virtual trip via the Internet to Virginia," Gov. Br. at 21 (internal citations and quotations omitted), that purported "trip" resulted in nothing more than a request to send information to a device in Colorado. *See* Warrant Aff., ¶ 33. And it was not until that information—including the government's malware—reached Colorado 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 a user's device and seizes control of that device.

CONCLUSION

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

---

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).

Dated: March 15, 2017

By: /s/ Mark Rumold

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

Counsel for Amicus Curiae

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 [6,430] 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: March 15, 2017

By: /s/ Mark Rumold
Mark Rumold

Counsel for Amicus Curiae

CERTIFICATE OF DIGITAL SUBMISSION

I hereby certify that with respect to the foregoing:

(1) all required privacy redactions have been made per 10th Cir. R. 25.5;

(2) if required to file additional hard copies, that the ECF submission is an exact copy of those documents;

(3) the digital submissions have been scanned for viruses with the most recent version of a commercial virus-scanning program, Avast Mac Security Version 12.5, updated February 14, 2017, and according to the program are free of viruses.

Dated: March 15, 2017

By: /s/ Mark Rumold
Mark Rumold

Counsel for Amicus Curiae

CERTIFICATE OF SERVICE

I hereby certify that I served the foregoing Brief of Amicus Curiae, on counsel for all parties, electronically through the Court's CM/ECF system, on this 15th day of March, 2017, which will send notification of such filing to counsel for all parties.

Dated: March 15, 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