NO. 17-30117

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

PLAINTIFF-APPELLEE,

V.

DAVID TIPPENS,

DEFENDANT-APPELLANT.

On Appeal from the United States District Court
for the Western District of Washington at Tacoma
Case No. 3:16-cr-05110-RJB-1
The Honorable Robert J. Bryan, Senior District Court Judge

BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT-APPELLANT

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

RULE 26.1 DISCLOSURE STATEMENT

Amicus curiae Electronic Frontier Foundation (EFF) is a non-profit public advocacy organization. EFF does not have a parent company, subsidiary or affiliate, and does not issue shares to the public.

Dated: October 20, 2017

By: /s/ *Mark Rumold*
Mark Rumold

ELECTRONIC FRONTIER FOUNDATION

Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Constitutional Provisions

STATEMENT OF INTEREST[1]

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 digital world since 1990. With over 38,000 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 in the First, Third, Fourth, Seventh, Eighth, and Tenth Circuits, as well as several district courts, in cases arising from the same investigation at issue in this appeal. *See United States v. Levin*, 16-1567 (1st Cir.); *United States v. Werdene*, 16-3588 (3rd Cir.); *United States v. Eure*, No. 17-4167 (4th Cir.); *United States v. Owens*, 17-1989 (7th Cir.); *United States v. Horton*, 863 F.3d 1041 (8th Cir. 2017); *United States v. Workman*, 863 F.3d 1313 (10th Cir. 2017).

---

[1] Pursuant to Federal Rule of Appellate Procedure 29(a)(2), amicus represents that no party objects to the filing of this brief. Pursuant to Federal Rule of Appellate Procedure 29(a)(4)(E), amicus states that no party or party's counsel has authored this brief in whole or in part, or contributed money that was intended to fund preparing or submitting the brief. No person has contributed money that was intended to fund preparing or submitting the brief.

INTRODUCTION

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

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

All of this was done based on a single warrant.

Instead of obtaining a narrowly tailored warrant, aimed at searching and 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, 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. Indeed, no court would seriously

consider a comparable warrant in the physical world. A warrant that authorized the search of thousands of 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.

The two circuit courts to decide appeals in these cases have both failed to address whether the warrant in this case was sufficiently particularized, mistakenly relying on the good faith exception from *United States v. Leon*, 468 U.S. 897 (1984). *See Workman*, 863 F.3d at 1317; *Horton*, 863 F.3d at 1049 & n.3. But the *Leon* exception does not apply to warrants that are deficient in precisely the manner of the warrant in this case, "i.e., in failing to particularize the place to be searched or the things to be seized." *Leon*, 468 U.S. at 923. To resolve this case—and the others in the Circuit like it—this Court can and should address the question of particularity, even if not squarely presented by the Appellant here.

Government hacking raises serious Fourth Amendment concerns—concerns exacerbated when the government cannot specifically identify or locate in advance the user or device it is hacking. *See In re Warrant to Search a Target Computer*, 958 F. Supp. 2d 753, 758-760 (S.D. Tex. 2013). To resolve this case, however, the Court need not conclusively answer whether hacking users or devices in unknown locations is per se unconstitutional. Instead, the Fourth Amendment question

presented here can be resolved more narrowly: by holding that a single warrant that fails to identify any user or device with any particularity cannot provide a constitutional basis to hack into thousands of electronic devices located around the world.

FACTUAL BACKGROUND

This case, like hundreds 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. ER_0040.

The Playpen investigation began with a tip from a foreign government. *See* Warrant Aff., ¶ 28.[2] 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

[2] Amicus understands that the warrant, its two incorporated attachments, and the warrant application and affidavit submitted by FBI Special Agent Douglas Macfarlane remain under seal in this case. Those documents have been made publicly available in other cases. *See, e.g.*, *United States v. Levin*, 15-cr-10271 (ECF No. 44-3) (D. Mass. Feb. 19, 2016). References herein to the "Warrant," "Warrant Attach." and the "Warrant Aff." are to those documents, respectively.

list of registered users, the actual IP addresses of many users, as well as logs of their activity on the site. *Id*., ¶¶ 29 & n.7, 30, 37.

I. 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 every day by millions of users around the world, including journalists, human rights advocates, lawyers, and governments—including the federal government.[3]

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 its users to circumvent software designed to censor content, to avoid tracking of their browsing behavior, and to facilitate other forms of anonymous communication.[4]

The Tor network consists of volunteer-operated computers, known as "nodes" or "relays," which enable Tor users to connect to websites "through a

---

[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. 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*.

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

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 network location of the site.[6] Other Tor users can connect to hidden services without knowing the site's actual network 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).

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

II. THE FBI'S USE OF MALWARE.

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]

---

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

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

During the two-week period the government operated Playpen, the FBI used malware, which they called a "Network Investigative Technique" (NIT), to infect the computers of users logging into the site. 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*.

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 malware used by identity thieves or other criminal "hackers."[8]

The NIT operated in 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*

---

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.

[8] Indeed, the NIT used here is similar to a class of malware known as a Remote Access Trojan ("RAT"), which often features 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.

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] When a visitor to the site logged in, computer code served by the government to the users' computers "exploited" one or more vulnerabilities in users' software to surreptitiously deliver and install the NIT.

2. Payload. Once resident on a user's 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 would not typically be disclosed to operators of a website on the Tor network.

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

---

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

[10] *See* Grimes, *supra* n.9.

computer's "Media Access Control" (MAC) address. See Warrant Attach. B.

3. Exfiltration of Data to the FBI. The NIT then transmitted the copied information back to the FBI. That information formed the basis for all further investigation in these cases. Ultimately, the FBI searched nearly 9,000 computers, located in over one hundred countries around the world in the manner described. ER_0040.[11]

ARGUMENT

The warrant was an unconstitutional general warrant because it lacks the careful tailoring and particularity the Fourth Amendment requires.

The Fourth Amendment requires that a warrant "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

---

[11] *See also* 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.

Fourth Amendment is unconstitutional." *Groh v. Ramirez*, 540 U.S. 551, 559-60 (2004) (internal quotations and citations omitted).

The warrant—which did not describe any particular person, place, or thing to search—theoretically authorized the search and seizure of an unlimited number of computers located anywhere in the world. Even narrowly construed, the warrant extended to hundreds of thousands of computers. And in practice, the FBI relied on the warrant to search nearly 9,000 computers in countries around the globe.

That, alone, should be dispositive.

Compounding matters, the absence of particularity in the warrant was unnecessary—both as a practical and technical matter. Even when compared to other types of constitutionally suspect warrants that push the boundaries of the particularity requirement, the warrant here is still more general. And this absence of particularity is especially troubling in light of the series of invasive searches and seizures carried out each time the FBI's malware was deployed.

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.

I. THE WARRANT VIOLATED THE FOURTH AMENDMENT BECAUSE IT FAILED TO PARTICULARLY DESCRIBE WHAT WAS BEING SEARCHED AND WHERE THOSE SEARCHES WOULD OCCUR.

The government obtained a single warrant that, on its face, authorized the search of at least 150,000 electronic devices located all over the world. Relying on that warrant, the FBI actually searched nearly 9,000 computers in over a hundred different countries. But the reach of the warrant was theoretically limitless—the FBI could search *any* computer accessing the site, no matter where that computer was located or the circumstances surrounding its logging in. That is the definition of a "virtual, all-encompassing dragnet" prohibited by the Fourth Amendment.

1. A single warrant to search upwards of 150,000 electronic devices, without specifying the location or providing a description 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. *United States v. Robertson*, 833 F.2d 777,783 (9th Cir. 1987) (finding warrant authorizing search of a residence insufficiently particularized to support a search of a backpack). Each person or place to be searched requires a specific description in the warrant—accompanied by an individualized showing of probable cause. *See Ybarra v. Illinois*, 444 U.S. 85, 91 (1979) ("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."); *see also Greenstreet v. Cnty. of San Bernardino*, 41

F.3d 1306, 1309 (9th Cir. 1994). Ultimately, particularity ensures that warrants are "confined in scope" and as limited as possible. *Voss v. Bergsgaard*, 774 F.2d 402, 404 (10th Cir. 1985).

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 at least 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, *see, e.g.*, ER_0040, the warrant, on its face, authorized FBI searches and seizures in every U.S. state and territory, indeed anywhere in the world.[12]

---

[12] The government's decision to conduct these searches—and the magistrate's decision to authorize them—raises special considerations for

In other words, the NIT warrant lacked particularity because it failed to identify with any specificity, which computers, out of all of the computers on earth, might be searched. *See In re Warrant to Search a Target Computer*, 958 F. Supp. 2d at 759.

2. The absence of particularity was not compelled by the technology at issue. Particularity 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. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1982) (noting validity of warrant turns on "whether the government was able to describe the items more particularly in light of the information available to it"); *United States v. Shi*, 525 F.3d 709, 731-32 (9th Cir. 2008). Although warrants may describe items in broad or generic terms, "[g]eneric classifications in a warrant are acceptable only when a more precise description is not possible." *United States v. Cardwell*, 680 F.2d 75, 78 (9th Cir. 1982), quoting *United States v. Bright*, 630 F.2d 804, 812 (5th Cir. 1980). 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. *United States v. Leary,* 846 F.2d 592, 600 (10th Cir. 1988) (internal quotations and citations omitted).

---

extraterritorial searches. *See Microsoft Corp. v. United States*, 829 F.3d 197, 212 (2d Cir. 2016).

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. 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 or identities 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 a theoretically limitless number of computers in locations across the globe.

It is thus by no means immaterial that the government could have provided additional detail in its application, thereby narrowing the scope of the warrant.

Such detail would have made 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. That 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.

II. OTHER TYPES OF CONSTITUTIONALLY-SUSPECT WARRANTS OFFER FAR MORE PARTICULARITY THAN THE WARRANT HERE.

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. As this Court and others have recognized, anticipatory warrants present "a potential for abuse above and beyond that which exists in more traditional settings." *United States v. Hotal*, 143 F.3d 1223, 1226 (9th Cir. 1998), quoting *United States v. Ricciardelli*, 998 F.2d 8, 12 (1st Cir. 1993).

Given this, the Supreme Court has recognized that, while anticipatory warrants are not "categorically unconstitutional," a valid anticipatory warrant requires 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). Without that showing, "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 establish, as *Grubbs* requires, the "likelihood that the condition w[ould] occur"—that a user would log into the website—for any specific computer or computer user (or, for that matter, any future registered user). On its face, then, the warrant authorized the search of *any* computer in the world, *if* that computer accessed Playpen, without establishing the likelihood of the event occurring for any one of them. That is functionally identical to the warrant the Supreme Court cautioned against in *Grubbs*.

Some courts have incorrectly found the NIT 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 that is no justification. The same logic could apply to an unconstitutional anticipatory warrant, conditioned on the delivery of contraband, for every house in the country, too. The warrant would still apply "only to" houses where the contraband was ultimately delivered. But this ignores *Grubbs*' requirement that there be a connection—established and described *at the time the warrant is sought*—between the triggering condition and a specific place to be searched. *Grubbs*, 547 U.S. at 96.

Indeed, no court would issue an analogous warrant in the physical world. For example, Seattle police undoubtedly have probable cause to believe the public sale of illegal drugs will occur in the city.[13] They can even point to particular locations—around Pike Place Market, 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.

---

[13] *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.").

But that is precisely what the warrant authorized here. The FBI was permitted to: (1) observe users as they attempted to access the website; (2) choose, at its discretion, which users to pursue; and (3) surreptitiously search 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 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[.]"). 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, 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 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).[14] In a departure from usual

[14] 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.

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. *See* 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.[15]

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 future event occurring at a particular place. But no constitutionally valid warrant can authorize the search of unnamed (and unlimited) persons in

---

Nevertheless, courts require stringent minimization of the conversations captured. *See Berger v. New York*, 388 U.S. 41, 56, 59 (1967).

[15] 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.

unnamed (and unlimited) places based upon the unsupported likelihood of a future event. Yet that is precisely what the warrant did here.

III. 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.

As the Supreme Court has recognized, the need for particularity is especially great in the case of electronic surveillance, like that at issue here. *See Berger v. New York*, 388 U.S. 41, 56 (1967). "By its very nature" electronic surveillance "involves an intrusion on privacy that is broad in scope," and the "indiscriminate use of such devices in law enforcement raises grave constitutional questions." *Id*.; *see also United States v. United States District Court for the Eastern District of Michigan*, 407 U.S. 297, 313 (1972) (warning against "broad and unsuspected incursions" into citizens' privacy that can be worked by electronic surveillance).

Here, each use of the FBI's malware triggered three distinct Fourth Amendment intrusions: (1) a forced 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. *See Berger*, 388 U.S. at 56 (electronic surveillance imposes "heavier responsibility" on courts to ensure fidelity to Fourth Amendment). 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 the 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)). It is no surprise, then, that courts uniformly recognize the need for warrants prior to searching computers. *See, e.g.*, *Horton*, 863 F.3d at 1047 (use of NIT required a warrant because defendant had a reasonable expectation of privacy in contents of his computer); *United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008); *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001).

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).

Some courts, including the court below, have improperly focused on the *information obtained* from the search (critically, the IP address), rather than *the place where the search occurred*. *See* ER_0050. The court below relied on this Court's decision in *United States v. Forrester*, 512 F.3d 500 (2008), which in turn relies on *Smith v. Maryland*, 442 U.S. 735 (1979)—all cases that concerned warrantless access to information in the possession of a *third party*.

Even 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 of privacy, that was not the case here. *See Horton,* 863 F.3d at 1046-47 ("This case differs from cases in which an IP address is voluntarily provided to third parties."). Instead, here, the government directly searched private areas on the user's computer without his knowledge or consent Thus, as the Eighth Circuit correctly concluded, a warrant was required. *Id*.

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 apparently agrees: the warrant itself described the copied information as the property "to be seized." See Warrant Attach. B.

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

CONCLUSION

"In this age of increasing government surveillance, lawful and unlawful . . . it is important that courts not grow lax in their duty to protect our right to privacy and that they remain vigilant against efforts to weaken our Fourth Amendment protections." *United States v. Gourde*, 440 F.3d 1065, 1074 (9th Cir. 2006) (en banc) (Reinhardt, J., *dissenting*).

This case is no exception. As law enforcement increasingly turns to

"hacking" the electronic devices of citizens as a tool for surveillance, it is imperative that appropriate Fourth Amendment limits are placed on the technique at the outset. For the reasons described above, this Court should find that the warrant the FBI relied on to hack thousands of computers located around the world violated the Fourth Amendment.

Dated: October 20, 2017

By: /s/Mark Rumold

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

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS PURSUANT TO FED. R. APP. P. 32(A)(7)(C)

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of Amicus Curiae Electronic Frontier Foundation In Support of Defendants-Appellants complies with the type-volume limitation, because this brief contains 5,751 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

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 this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2011, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: October 20, 2017

By: /s/ *Mark Rumold*
Mark Rumold

Counsel of Record for Amicus Curiae

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on October 20, 2017.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: October 20, 2017

By: /s/ *Mark Rumold*
Mark Rumold

Counsel of Record for Amicus Curiae