No. 17-4299

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,

PLAINTIFF-APPELLEE,

v.

ROBERT MCLAMB,

DEFENDANT-APPELLANT.

On Appeal from the United States District Court
for the Eastern District of Virginia, Norfolk Division
Case No. 2:16-cr-00092-RBS
The Honorable Rebecca Beach Smith, United States District Court Judge

BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION AND THE NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS IN SUPPORT OF DEFENDANT-APPELLANT

Cindy Cohn
Counsel of Record
Mark Rumold
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
cindy@eff.org

Counsel for Amicus Curiae EFF

Elizabeth Franklin-Best
NATIONAL ASSOCIATION OF
CRIMINAL DEFENSE LAWYERS
Blume Franklin-Best & Young, LLC
900 Elmwood Avenue, Suite 200
Columbia, South Carolina 29201
(803) 765-1044

Counsel for Amicus Curiae NACDL

DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION

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

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

TABLE OF CONTENTS

TABLE OF CONTENTS iii

TABLE OF AUTHORITIES iv

STATEMENT OF INTEREST 1

INTRODUCTION 3

FACTUAL BACKGROUND 5

A. Tor. 5

B. The FBI's use of malware. 7

ARGUMENT 10

I. The warrant failed to particularly describe what was being searched and where those searches would occur. 11

II. Particularity was critical given the series of invasive searches and seizures carried out each time the malware was deployed. 15

III. Other constitutionally suspect types of warrants offer far more particularity than the warrant here. 20

CONCLUSION 25

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS PURSUANT TO FED. R. APP. P. 32(A)(7)(C) 27

TABLE OF AUTHORITIES

Cases

Berger v. New York,
388 U.S. 41 (1967).....15, 16, 24

Boyd v. United States,
116 U.S. 616 (1886).....18

Coolidge v. New Hampshire,
403 U.S. 443 (1971).....10

Go-Bart Importing Co. v. United States,
282 U.S. 344 (1931).....10

Groh v. Ramirez,
540 U.S. 551 (2004).....10

Illinois v. Gates,
462 U.S. 213 (1983).....22

In re Warrant to Search a Target Computer,
958 F. Supp. 2d 753 (S.D. Tex. 2013).....4, 13

Katz v. United States,
389 U.S. 347 (1967).....17

LeClair v. Hart,
800 F.2d 692 (7th Cir. 1986).....19

Marks v. Clarke,
102 F.3d 1012 (9th Cir. 1996).....23

Microsoft Corp. v. United States,
829 F.3d 197 (2d Cir. 2016).....13

Mongham v. Soronen,
2013 WL 705390 (S.D. Ala. Feb. 26, 2013).....23

Rakas v. Illinois,
439 U.S. 128 (1978).....18

Riley v. California,
134 S. Ct. 2494 (2014).....18

Smith v. Maryland,
442 U.S. 735 (1979).....19

Stanford v. Texas,
379 U.S. 476 (1965).....4

State v. De Simone,
288 A.2d 849 (N.J. 1972) 23

Trulock v. Freeh,
275 F.3d 391 (4th Cir. 2001) 18

United States v. Am. Investors of Pittsburgh, Inc.,
879 F.2d 1087 (3d Cir. 1989) 13

United States v. Andrews,
577 F.3d 231 (4th Cir. 2009) 20

United States v. Anzalone,
15-cr-10347 (D. Mass. Sep. 22, 2016).....21

United States v. Arterbury,
15-cr-0018 (N.D. Ok. filed Apr. 25, 2016).....17

United States v. Bridges,
344 F.3d 1010 (9th Cir. 2003) 11

United States v. Bright,
630 F.2d 804 (5th Cir. 1980) 13, 14

United States v. Carlson,
No. 16-cr-317 (D. Minn. Mar. 23, 2017).....13, 22

United States v. Comprehensive Drug Testing, Inc.,
621 F.3d 1162 (9th Cir. 2010) 19

United States v. Cotterman,
709 F.3d 952 (9th Cir. 2013) 18

United States v. Croghan,
209 F. Supp. 3d 1080 (S.D. Iowa 2016) 19

United States v. Darby,
190 F. Supp. 3d 520 (E.D. Va. 2016) 18

United States v. Grubbs,
547 U.S. 90 (2006).....20, 21

United States v. Guadarrama,
128 F. Supp. 2d 1202 (E.D. Wis. 2001).....23

United States v. Heckenkamp,
482 F.3d 1142 (9th Cir. 2007) 18

United States v. Hurwitz,
459 F.3d 463 (4th Cir. 2006) 12

United States v. Jackson,
207 F.3d 910 (7th Cir. 2000) 24

United States v. Jacobsen,
466 U.S. 109 (1984).....17, 19

United States v. Jones,
565 U.S. 400 (2012).....17, 24

United States v. Leary,
846 F.2d 592 (10th Cir. 1988) 13, 14, 15

United States v. Petti,
973 F.2d 1441 (9th Cir. 1992) 24

United States v. Silberman,
732 F. Supp. 1057 (S.D. Cal. 1990).....24

United States v. Stabile,
633 F.3d 219 (3d Cir. 2011) 18

United States v. Tippens,
No. 16-05110-RJB (W.D. Wash. Nov. 30, 2016).....5, 9, 13

United States v. Torch,
609 F.2d 1088 (4th Cir. 1979) 12, 13

United States v. United States District Court for the Eastern District of Michigan,
407 U.S. 297 (1972).....16

United States v. Werdene,
188 F. Supp. 3d 431 (E.D. Pa. 2016).....18

United States v. Williams,
592 F.3d 511 (4th Cir. 2010) 14

Voss v. Bergsgaard,
774 F.2d 402 (10th Cir. 1985) 12

Wallace v. King,
626 F.2d 1157 (4th Cir. 1980) 4

Ybarra v. Illinois,
444 U.S. 85 (1979).....12, 23

Statutes

18 U.S.C. § 2518(11) 24

Constitutional Provisions

U.S. Const. amend. IV.....*passim*

Other Authorities

Joseph Cox, *The FBI Hacked Over 8,000 Computers In 120 Countries Based on One Warrant*, Motherboard, Nov. 22, 2016 9

Roger A. Grimes, *Danger: Remote Access Trojans*, Microsoft TechNet (Sept. 2002).....8, 9

Wayne R. LaFave, *Search and Seizure* (4th ed. 2004) 10, 20

Malware Protection Center, Microsoft.....8

Robert Moir, *Defining Malware: FAQ*, Microsoft TechNet (Oct. 2003) 7

Murugiah Souppaya & Karen Scarfone, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, NIST Special Publication (July 2013) 7

Tor and HTTPS, EFF 6

Tor Project, Inception.....6

Tor Project, Sponsors 6

Tor: Hidden Service Protocol.....7

STATEMENT OF INTEREST[1]

Amicus curiae Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world since 1990. With over 36,000 active donors, EFF represents technology users' interests in court cases and broader policy debates involving the Fourth Amendment and its relationship to technology and new surveillance techniques. Relevant here, EFF has participated as amicus in the First, Third, Eighth, and Tenth Circuits, as well as two district courts, in cases arising from the same investigation at issue here. *See United States v. Levin*, 16-1567 (1st Cir.); *United States v. Werdene*, 16-3588 (3rd Cir.); *United States v. Croghan*, Nos. 16-3976, 16-3982 (8th Cir.); *United States v. Workman*, No. 16-1401 (10th Cir.); *see also United States v. Matish*, No. 16-cr-0016 (E.D. Va.); *United States v. Owens*, 16-cr-0038 (E.D. Wisc.).

The National Association of Criminal Defense Lawyers (NACDL) is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. NACDL was founded in 1958. It has a nationwide membership of many thousands of direct members, and up to 40,000 with affiliates. NACDL's

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

members include private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges. NACDL is the only nationwide professional bar association for public defenders and private criminal defense lawyers. NACDL is dedicated to advancing the proper, efficient, and just administration of justice. NACDL files numerous amicus briefs each year in the U.S. Supreme Court and other federal and state courts, seeking to provide amicus assistance in cases that present issues of broad importance to criminal defendants, criminal defense lawyers, and the criminal justice system as a whole. NACDL has a particular interest in robust Fourth Amendment protections in the digital age.

Amici filed a substantively identical brief before this Court in *United States v. Eure*, 17-4167 (4th Cir.)—a case arising from the same investigation at issue here.

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 limits the Fourth Amendment places on this new technique.

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

All of this was done based on a single warrant.

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

Instead of obtaining a narrowly tailored warrant, aimed at 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); *cf. Wallace v. King*, 626 F.2d 1157, 1160 (4th Cir. 1980).

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). But to resolve this case, 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, fails to provide a constitutional basis to hack into thousands of electronic devices located around the world.

As explained in more depth below, the warrant in this case was a general one, and it therefore violated the Fourth Amendment.

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, it had access to all the data and other information on the server, including a list of registered users, as well as logs of their activity on the site. *Id*., ¶¶ 29, 30, 37.

A. Tor.

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

---

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

[3] The warrant, its two incorporated attachments, and the warrant application and affidavit submitted by FBI Special Agent Douglas Macfarlane, are available at J.A. 48-84. References herein to the "Warrant," "Warrant Attach." or the "Warrant Aff." are to those documents, respectively.

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.[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 its users to circumvent software designed to censor content, to avoid tracking of their browsing behavior, and to facilitate other forms of anonymous communication.[5]

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

---

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

[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.

Using Tor, individuals can also host websites known as "hidden services," which do not reveal the network location of the site.[7] Other Tor users can connect to hidden services without knowing the site's actual 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.

B. 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.[8]

During the two-week period the government operated Playpen, the FBI used malware, which they called a "Network Investigative Technique" (NIT), to infect

---

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

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

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."[9]

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* 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 users' computers relied on one or

---

[9] 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.

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

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.[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.

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.

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.[12]

---

[11] *See* Grimes, *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, 2016,

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 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 or place—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 located in over one hundred different countries. Those facts, alone, should be dispositive. Yet the absence of particularity

---

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

was compounded, both by the government's ability to obtain a more narrow warrant and the series of invasive searches and seizures that resulted each time the government used this technique. Ultimately, even other constitutionally suspect warrants have far more particularity than the warrant here.

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 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. The FBI actually searched nearly 9,000 computers in over one-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 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. *United States v. Torch*, 609 F.2d 1088, 1090 (4th Cir. 1979). 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 United States v. Hurwitz*, 459 F.3d 463, 473 (4th Cir. 2006). Ultimately, particularity ensures that warrants are "confined in scope." *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, the warrant, on its face, authorized FBI searches and seizures in every U.S. state and territory, indeed anywhere in the world.[13] As one court explained, "the NIT warrant lacks particularity" because it failed to "identify with any specificity, which computers, out of all of the computers on earth, might be searched pursuant to this warrant." Report & Recommendation at 23, *United States v. Carlson*, No. 16-cr-317 (D. Minn. Mar. 23, 2017) (ECF No. 44) ("*Carlson* R&R"); *see also In re Warrant to Search a Target Computer*, 958 F. Supp. 2d 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. *See Torch*, 609 F.2d at 1090; *see also United States v. Am. Investors of Pittsburgh, Inc.*, 879 F.2d 1087, 1106 (3d Cir. 1989) (citing *United States v. Leary,* 846 F.2d 592 (10th Cir. 1988)). Although warrants may describe items in broad or generic terms, "generic classifications in a warrant are acceptable only when a more precise description is not possible." *United States v. Bright*, 630

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

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. *Leary,* 846 F.2d at 600 (internal quotations and citations omitted); *see also United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010) (particularity is satisfied "when the description of the items leaves nothing to the discretion of the officer executing the warrant").

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. *See* J.A. 68-69, 525, 586.

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. 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.

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

Given the significant Fourth Amendment events that occurred each time the government deployed its malware, a specific and particularized warrant was crucial. *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.*, *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001); *United States v. Stabile*, 633 F.3d 219, 232 (3d Cir. 2011); *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007). Thus, a user's personal computer is a private area subject to the user's reasonable expectation of privacy. *See United States v. Darby*, 190 F. Supp. 3d 520, 528-530 (E.D. Va. 2016).

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).[14]

[14] Some courts have improperly focused on the *information obtained* from the search rather than *the place where the search occurred*. *See, e.g.*, *United States v. Werdene*, 188 F. Supp. 3d 431, 444 (E.D. Pa. 2016). But these analyses rely on

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

---

Smith v. Maryland, 442 U.S. 735 (1979), and its progeny, which 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. Rather, here, the government directly searched private areas on the user's computer, without his knowledge or consent. *See United States v. Croghan*, 209 F. Supp. 3d 1080, 1092-93 (S.D. Iowa 2016) (noting the "significant difference between obtaining an IP address from *a third party* and obtaining it *directly from a defendant's computer*") (emphasis in original).

computer, that copying constituted a Fourth Amendment seizure.

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

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

1. The warrant in this case was a species of constitutionally suspect warrant known as an "anticipatory warrant." An anticipatory warrant is based on "probable cause that at some future time (but not presently) certain evidence of a crime will be located at a specified place," 2 LaFave, *Search and Seizure* § 3.7(c), p. 398. Although not "categorically unconstitutional," anticipatory warrants 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); *see United States v. Andrews*, 577 F.3d 231, 237 (4th Cir. 2009) (quoting *Grubbs*). Were that not the case, "an anticipatory warrant could be issued for every house in the country, authorizing search and seizure *if* contraband should be delivered—though for any single location there is no likelihood that contraband will be delivered." *Id*. at 96 (emphasis in original).

The warrant here was unquestionably anticipatory. The search and seizure of an "activating computer" was predicated on a user logging into Playpen at some unspecified point in the future. *See* Warrant at 2; *see also* J.A. 687-88 (recognizing warrant was based on triggering condition).

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, *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 warned against in *Grubbs*. *See id*.

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 that could be said of a warrant for every house in the country, too: the warrant would only apply to houses where contraband was delivered. This conclusion thus 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; *see also Carlson* R&R at 26.

Indeed, no court would issue an analogous warrant in the physical world. For example, Richmond police undoubtedly have probable cause to believe the public sale of illegal drugs will occur in the city.[15] They can even point to particular locations—outside a concert at the National Theater, for example—where sales are likely to occur. Yet no court would issue an anticipatory warrant that authorized the police to: (1) observe such public sales, (2) decide which suspects to pursue, and (3) subsequently (and surreptitiously) enter purchasers' homes in order to identify them.

Yet that is precisely what the warrant authorized here. The FBI was 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

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

than the warrant here.

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

Even assuming their constitutionality as a general class, amici are not aware of an "all persons" warrant that comes close to approximating the reach of the warrant here. First, "all persons" warrants are by definition tied to the search of a particular physical location—something conspicuously absent here. Second, "all persons" warrants are necessarily limited by physical constraints. These warrants authorize searches of a small number of people physically present at a specific location. *See State v. De Simone*, 288 A.2d 849, 853 (N.J. 1972) (collecting cases in which 10-30 individuals were searched). In contrast, here, the warrant

authorized searches of over a hundred thousand users' devices in locations around the world. No comparable "all persons" warrant has ever issued. *See Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (noting electronic surveillance evades "ordinary checks" on abuse, including limited police resources)

3. Finally, warrants for roving wiretaps—yet another species of suspect warrant—permit interception of a *particular, identified* suspect's communications, even where the government cannot identify in advance the particular facilities that the suspect will use. *See, e.g., United States v. Petti*, 973 F.2d 1441, 1444-46 (9th Cir. 1992); *United States v. Jackson*, 207 F.3d 910, 914 (7th Cir. 2000), *vacated on other grounds by* 531 U.S. 953 (2000) (citing cases).[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. *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, though the government could have done so. Instead, the government sought authorization to search *anyone* accessing the site. Nor is this a case where Congress has established a specific surveillance framework imposing additional safeguards in the face of constitutional uncertainty. Instead, the government made up rules—broad ones—as it went along.

* * *

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

CONCLUSION

For the reasons described above, the warrant violated the Fourth Amendment.

Dated: June 27, 2017

Respectfully submitted,

/s/ Cindy Cohn
Cindy Cohn
Counsel of Record

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

Counsel for Amicus Curiae Electronic Frontier Foundation

Elizabeth Franklin-Best
NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
Blume Franklin-Best & Young, LLC
900 Elmwood Avenue, Suite 200
Columbia, South Carolina 29201
(803) 765-1044

Counsel for Amicus Curiae National Association of Criminal Defense Lawyers

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 *Amici Curiae* complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 5,611 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: June 27, 2017

/s/ Cindy Cohn
Cindy Cohn

Counsel of Record for Amici Curiae

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

APPEARANCE OF COUNSEL FORM

BAR ADMISSION & ECF REGISTRATION: If you have not been admitted to practice before the Fourth Circuit, you must complete and return an Application for Admission before filing this form. If you were admitted to practice under a different name than you are now using, you must include your former name when completing this form so that we can locate you on the attorney roll. Electronic filing by counsel is required in all Fourth Circuit cases. If you have not registered as a Fourth Circuit ECF Filer, please complete the required steps at Register for eFiling.

THE CLERK WILL ENTER MY APPEARANCE IN APPEAL NO. 17-4299 as

☐ Retained ☐ Court-appointed(CJA) ☐ Court-assigned(non-CJA) ☐ Federal Defender ☑ Pro Bono ☐ Government

COUNSEL FOR: Electronic Frontier Foundation

_____ as the
(party name)

☐ appellant(s) ☐ appellee(s) ☐ petitioner(s) ☐ respondent(s) ☑ amicus curiae ☐ intervenor(s) ☐ movant(s)

/s/ Cindy Cohn
(signature)

Cindy Cohn
Name (printed or typed)

(415) 436-9333
Voice Phone

Electronic Frontier Foundation
Firm Name (if applicable)

(415) 436-9993
Fax Number

815 Eddy Street

San Francisco, CA 94109
Address

cindy@eff.org
E-mail address (print or type)

CERTIFICATE OF SERVICE

I certify that on 6/27/2017 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

/s/ Cindy Cohn
Signature

6/27/2017
Date