IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN
MILWAUKEE DIVISION

UNITED STATES OF AMERICA	:	
	:	
Plaintiff,	:	**Case No. 16-cr-38**
v.	:	
	:	**Hon. J.P. Stadtmueller**
MARCUS A. OWENS	:	
	:	**ELECTRONICALLY FILED**
Defendant.		

BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT

Christopher Donovan
PRUHS & DONOVAN, S.C.
757 N. Broadway, Suite 401
Milwaukee, Wisconsin 53202
Phone: (414) 221-1950
Fax: (414) 221-1959
donovanc34@hotmail.com

Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF CONTENTS ii

TABLE OF AUTHORITIES iii

INTRODUCTION 1

FACTUAL BACKGROUND 3

I. Tor 3

III. Law Enforcement's Investigation of Playpen 5

ARGUMENT 7

I. The Warrant Is an Unconstitutional General Warrant. 7

A. Each deployment of the FBI's malware resulted in a series of invasive searches and seizures. 7

1. The presence of government malware on a user's device is a Fourth Amendment seizure. 8

2. Operating malware on a user's computer is a Fourth Amendment search. 8

3. Copying data from a computer is a Fourth Amendment seizure. 12

B. The Warrant lacked particularity and was therefore invalid. 12

1. The Government could have provided additional information in the Warrant—but chose not to. 13

2. The Warrant failed to particularly describe what was being searched and where those searches would occur. 15

3. The Warrant vested too much discretion in the executing officers. 16

4. The Warrant exceeds even other constitutionally suspect warrants, including roving wiretaps, "all persons" warrants, and anticipatory warrants. 18

II. Complying with the Fourth Amendment Does Not Create an Insurmountable Bar for Law Enforcement, Even in Cases Like This. 21

CONCLUSION 22

TABLE OF AUTHORITIES

Cases

Arizona v. Evans,
514 U.S. 1 (1995) 21

Berger v. New York,
388 U.S. 41 (1967) 1, 18

Boyd v. United States,
116 U.S. 616 (1886) 9

Coolidge v. New Hampshire,
403 U.S. 443 (1971) 12, 17

Go-Bart Importing Co. v. United States,
282 U.S. 344 (1931) 13

Greenstreet v. Cnty. of San Bernardino,
41 F.3d 1306 (9th Cir. 1994) 15

Groh v. Ramirez,
540 U.S. 551 (2004) 17

Jones v. Wilhelm,
425 F.3d 455 (7th Cir. 2005) 14

Katz v. United States,
389 U.S. 347 (1967) 9, 17

Kyllo v. United States,
533 U.S. 27 (2001) 11

LeClair v. Hart,
800 F.2d 692 (7th Cir. 1986) 12

Marks v. Clarke,
102 F.3d 1012 (9th Cir. 1996) 19

Marron v. United States,
275 U.S. 192 (1927) 16

Maryland v. Garrison,
480 U.S. 79 (1987) 14

Massachusetts v. Sheppard,
468 U.S. 981 (1984) 13

Microsoft Corp. v. United States,
No. 14 - 2985, 2016 WL 3770056 (2d Cir. July 14, 2016) 12, 16

Mongham v. Soronen,
2013 WL 705390 (S.D. Ala. Feb. 26, 2013) 19

Payton v. New York,
445 U.S. 573 (1980) 21

Rakas v. Illinois,
439 U.S. 128 (1978) 9, 11

Riley v. California,
134 S. Ct. 2473 (2014) 9, 10, 11

State v. De Simone,
60 N.J. 319 (N.J. 1972) 19

Smith v. Maryland,
442 U.S. 735 (1979) 11

Stanford v. Texas,
379 U.S. 476 (1965) 1, 2, 16

Steagald v. United States,
451 U.S. 204 (1981) 15

Trulock v. Freeh,
275 F.3d 391 (4th Cir. 2001) 10

United States v. Andrus,
483 F.3d 711 (10th Cir. 2007) 9

United States v. Arterbury,
15-cr-0018 (N.D. Ok. filed Apr. 25, 2016) 8

United States v. Bridges,
344 F.3d 1010 (9th Cir. 2003) 16, 17

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

United States v. Brown,
832 F.2d 991 (7th Cir. 1987) 13

United States v. Cardwell,
680 F.2d 75 (9th Cir. 1982) 13

United States v. Comprehensive Drug Testing, Inc.
621 F.3d 1162 (9th Cir. 2010) 12, 17

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

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

United States v. Guadarrama,
128 F. Supp. 2d 1202 (E.D. Wis. 2001) 19

United States v. Jackson,
207 F.3d 910 (7th Cir. 2000) 18

United States v. Jacobsen,
466 U.S. 109 (1984) 8, 12

United States v. Jefferson,
571 F. Supp. 2d 696 (E.D. Va. 2008) 12

United States v. Jones,
132 S. Ct. 945 (2012) 1, 8, 19

United States v. Jones,
54 F.3d 1285 (7th Cir. 1995) 13, 14

United States v. Lambis,
No 15-cr-734, 2016 WL 3870940 (S.D.N.Y. July 12, 2016) 11

United States v. Levin,
No. 15-10271-WGY, 2016 WL 2596010 (D. Mass. May 5, 2016) 5, 6

United States v. Matish,
No. 16-cr-16, 2016 WL 3545776 (E.D. Va. June 23, 2016) 7, 10, 11, 14

United States v. Payton,
573 F.3d 859 (9th Cir. 2009) 9

United States v. Petti,
973 F.2d 1441 (9th Cir. 1992) 18

United States v. Silberman,
732 F. Supp. 1057 (S.D. Cal. 1990) 18

United States v. Sims,
553 F.3d 580 (7th Cir. 2009) 15, 16

United States v. Spilotro,
800 F.2d 959 (9th Cir. 1986) 14

United States v. Werdene,
No. 15-cr-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016) 11

Virginia v. Moore,
553 U.S. 164 (2008) 2

Walter v. United States,
447 U.S. 649 (1980) 15

Ybarra v. Illinois,
444 U.S. 85 (1979) 19

Statutes

18 U.S. Code § 2518(11) 18

Other Authorities

BlackShades: Arrests in Computer Malware Probe, BBC (May 19, 2014) 4

FBI, "*Three Men Arrested in Hacking and Spamming Scheme*," (Dec. 15, 2015) 5

Jemima Kiss, *Privacy tools used by 28% of the online world, research finds*,
Guardian (Jan. 21, 2014) 3

Joseph Cox, *New Case Suggests the FBI Shared Data from Its Mass Hacking Campaign with the UK*, Motherboard (Feb. 10, 2016) 16

Malware Analysis - Dark Comet RAT, Context, (Nov. 2, 2011) 4

Robert Moir, *Defining Malware: FAQ*, Microsoft TechNet (Oct. 2003) 4

Roger A. Grimes, *Danger: Remote Access Trojans*, Microsoft TechNet (Sept. 2002) 4

The Tor Project 3

Tor and HTTPS, EFF 3

Tor: Hidden Service Protocol 4

Wayne R. LaFave, *Search and Seizure* (Thomson/West, 4th ed. 2004) 12, 20

INTRODUCTION

The Internet has fundamentally altered how we work, communicate, and share ideas. It represents the most significant contribution to the dissemination of speech since the printing press. Yet it is also a remarkably fragile ecosystem, one vulnerable to censorship and, as it has currently developed, surveillance. Much of what Internet users do every day is tracked by multiple parties—service providers, advertisers, governments and others, sometimes all at once.

Tor—a network and a software system central to the motions before the Court—was developed in response to this surveillance. Tor represents the best attempt yet at affording some genuine level of privacy and anonymity to Internet users. Human rights advocates use Tor to avoid scrutiny from authoritarian regimes; journalists use Tor to communicate with anonymous sources; corporations use Tor to protect business strategy, and so on. Even governments (including the federal government) use Tor.

It is undisputed that criminals can also use Tor's privacy-enhancing technologies. But when law enforcement encroaches on Tor users' privacy, it must be done carefully and under narrowly defined circumstances. This is so for two reasons:

First, electronic surveillance, "[b]y its very nature . . . involves an intrusion on privacy that is broad in scope." *Berger v. New York*, 388 U.S. 41, 56 (1967). The surreptitious nature of electronic surveillance "evades the ordinary checks that constrain abusive law enforcement practices." *United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring). As such, careful judicial scrutiny is imperative. *See Berger*, 388 U.S. at 56.

Second, when law enforcement actions implicate First Amendment concerns—like anonymity and the dissemination of speech online—the requirements of the Fourth Amendment must be satisfied with "scrupulous exactitude." *Stanford v. Texas*, 379 U.S. 476, 485 (1965).

The warrant the government sought in this case did not approach the kind of "scrupulous

exactitude" the Constitution requires. In this case, and numerous others arising from the same investigation, the government obtained a single warrant authorizing it to surreptitiously place code on an unlimited number of computers, to search those computers, and to extract information from them. On its face, the warrant—which did not describe any particular person or place—authorized the search and seizure of data from hundreds of thousands of computers located around the world. Those two facts, alone, are sufficient to render the warrant invalid.

Moreover, the use of the Tor network did not require the government to seek a warrant as sweeping as the one it obtained. The government was in control of the server that hosted the targeted website. That control gave the government a wealth of information about the site, its individual users, and their individual activity. Accordingly, this is not a case where the government pursued all available avenues of investigation prior to seeking a generalized warrant. Nor was it unable to provide the magistrate with more information about particular targets of investigation. Instead, the government sought—and received—authorization to cast its electronic net as broadly as possible.

But the dragnet ran afoul of the Fourth Amendment's requirements. "The immediate object of the Fourth Amendment was to prohibit the general warrants and writs of assistance that English judges had employed against the colonists[.]" *Virginia v. Moore*, 553 U.S. 164, 168-69 (2008). Its words "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*, 379 U.S. at 481.

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

FACTUAL BACKGROUND

I. Tor

Tor began as a project of the United States Naval Research Lab in the 1990s.[1] Recognizing the privacy enhancing value of the technology, *amicus curiae* EFF provided financial support for Tor in 2004 and 2005.[2] The Tor Project is now an independent non-profit.[3] The Project's primary responsibility is maintaining the Tor network (or, generally, "Tor")—"a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet."[4]

Tor consists of a computer network and software that work together to provide Internet users with anonymity when they go online. Tor works by obscuring aspects of how and where its users are accessing the Internet, allowing users to circumvent software designed to censor content, to avoid tracking of their browsing behaviors, and to facilitate other forms of anonymous communication.[5] According to reports, as of 2014, "11% of all [Internet] users claim to use Tor," and Tor "could be regularly used by as many as 45.13 million people."[6]

To connect to the Tor network, users download and run Tor software on their devices. The Tor network consists of computers, known as "nodes" or "relays," operated by volunteers, which make it possible for users running the Tor software to connect to websites "through a series of virtual tunnels rather than making a direct connection."[7] This allows Tor users to share

---

[1] Inception, *available at* https://www.torproject.org/about/torusers.html.en
[2] Tor Sponsors, *available at* https://www.torproject.org/about/sponsors.html.en
[3] Core Tor People, *available at* https://www.torproject.org/about/corepeople
[4] Tor: Overview, *available at* https://www.torproject.org/about/overview.html.en.
[5] *Id.*
[6] Jemima Kiss, *Privacy tools used by 28% of the online world, research finds*, Guardian (Jan. 21, 2014), *available at* http://www.theguardian.com/technology/2014/jan/21/privacy-tools-censorship-online-anonymity-tools.
[7] *See* Tor Overview, *supra* n.4. For a visual representation of how Tor works to protect web traffic, *see Tor and HTTPS*, EFF, *available at* https://www.eff.org/pages/tor-and-https.

information over public Internet networks without compromising their privacy.

Using Tor, individuals can also host websites known as "hidden services," which do not reveal the location of the site.[8] Tor users can then connect to these hidden services, even without knowing the location of the site and without the site knowing its visitors' locations.

II. Government Use of Malware and Exploitation of Software Vulnerabilities

Malware is short for "malicious software" and is typically used as a catch-all term to refer to any software designed to disrupt or damage computer operations, gather sensitive information, gain unauthorized access, or display unwanted advertising.[9]

Relevant here is a specific type of malware known as a Network Investigative Technique ("NIT").[10] NITs are delivered to the target computer by taking advantage of unknown, obscure, or otherwise unpatched flaws in software running on the target computer. Exploiting these software flaws allows the attacker to control a device or extract data without the knowledge or consent of the owner of the target computer.[11] NITs share some capabilities with other similar, non-governmental software known as Remote Administration Tools ("RATs"), which often include "keystroke logging, file system access and remote control; including control of devices such as microphones and webcams."[12]

The government has objected to comparisons of a NIT to a RAT or malware, as well as to using the term "hacking" to describe its use of NITs, but these terms are commonly used in the

---

[8] *See generally* Tor: Hidden Service Protocol, *available at* https://www.torproject.org/docs/hidden-services.html.en.
[9] *See* Robert Moir, *Defining Malware: FAQ*, Microsoft TechNet (Oct. 2003), *available at* https://technet.microsoft.com/en-us/library/dd632948.aspx.
[10] *See* Roger A. Grimes, *Danger: Remote Access Trojans*, Microsoft TechNet (Sept. 2002), *available at* https://technet.microsoft.com/en-us/library/dd632947.aspx; *BlackShades: Arrests in Computer Malware Probe*, BBC (May 19, 2014), http://www.bbc.com/news/uk-27471218.
[11] *Malware Analysis - Dark Comet RAT*, Context, (Nov. 2, 2011), http://www.contextis.com/resources/blog/malware-analysis-dark-comet-rat/.
[12] *Id.*

technical community to describe surreptitious behavior like the government's here. In the government's view, while "hacking" may involve the exploitation of software vulnerabilities and the use of similar software to extract information from unsuspecting users, *its* exploitation of vulnerabilities and extraction of information is not malicious because it is "authorized," in the sense that a court sanctioned its use. Hackers use RATs to extract sensitive information, such as financial information, photos, and personal communications, from a computer;[13] much in the same way the FBI used its NIT in this case to extract private information from users' computers without their knowledge.

III. Law Enforcement's Investigation of Playpen

EFF understands that this case arises from the same set of facts as *United States v. Levin*, No. 15-10271-WGY, 2016 WL 2596010, at *2 (D. Mass. May 5, 2016), which describes a law enforcement investigation of Playpen, a website hosting child pornography, and the visitors to the site, all based on a single warrant issued in the Eastern District of Virginia (the "Warrant"). While some of the details of the technology involved have not been disclosed by the government, enough information is in the public record to understand how the investigation proceeded.

According to the government, it took physical possession of the server or servers that hosted Playpen and assumed the role of website administrator for a two-week period. *Id.* 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. *See id.*

Playpen operated as a Tor hidden service. Aff. in Supp. of Warrant at 12, Ex. 3 to Def.'s Mot. to Suppress, *Levin* (ECF No. 44-3) ("Aff. in Supp. of Warrant"). As noted above, in its normal mode of operation, the operators of a Tor hidden service do not have access to

[13] *See* FBI, "*Three Men Arrested in Hacking and Spamming Scheme*," (Dec. 15, 2015), https://www.fbi.gov/newark/press-releases/2015/three-men-arrested-in-hacking-and-spamming-scheme.

identifying details—such as the IP addresses—of visitors to the site. *Id*. at 22. In the course of its investigation, during the period while the government was operating Playpen, investigators used malware to infect the computers of users who logged into the site. *Levin*, 2016 WL 2596010, at *2. That malware allowed the government to defeat the anonymity features of the Tor network by searching infected computers for specific, identifying information and relaying that information back to the FBI. *Id*.

It appears from the government's brief that it employed at least two different delivery methods for its malware for different users of the site. Aff. in Supp. of Warrant at 24 n.8. From the publicly available information, it appears that for some target users, "such as those who attained higher status on the website," the government employed a more sophisticated delivery method for the malware—one that used a different, less detectable vulnerability to infect users' computers. *Id.*

But the operation of the malware was similar, regardless of its method of delivery: Code served by the government to the target computers used one or more vulnerabilities in the users' software in order to install the NIT. The NIT then searched a user's computer and extracted private, identifying data (a MAC address, operating system username, and other related information) that operators of websites on the Tor network do not otherwise have access to. That seized information was then sent back unencrypted to the FBI. The FBI noted the Internet Protocol (IP) address associated with this transmission, concluding that this IP address corresponded to the target computer.[14] The information in the NIT's transmission as well as the

[14] The Affidavit in support of the NIT warrant stated it would collect (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" address. See Aff. in Supp. of

associated IP address formed the basis for all subsequent investigation in this case.

ARGUMENT

I. The Warrant Is an Unconstitutional General Warrant.

The Warrant issued in this case lacked careful tailoring and particularity. In fact, as far as EFF is aware, the Warrant is unprecedented in its breadth and the discretion it granted to the officials executing it. That breadth is underscored by the significance of the activities it authorized the FBI to perform: surreptitiously infecting an individual's software and computer with government malware, searching the computer, and then copying data from that computer.

The Warrant represents a serious departure from traditional Fourth Amendment jurisprudence. As such, it more closely approximates the general warrants and writs of assistance the Fourth Amendment was designed to prevent, rather than the narrowly tailored and focused authorization to search and seize contemplated by the Fourth Amendment's drafters.

A. Each deployment of the FBI's malware resulted in a series of invasive searches and seizures.

The Warrant glosses over the significant Fourth Amendment events that occurred *each time* the government deployed its malware. Each use of the NIT triggered three Fourth Amendment events: (1) an entry into and seizure of the user's computer; (2) a search of the private areas of that computer; and (3) a seizure of private information from the computer.

That two seizures and a search occurred each time the malware was deployed is evidence of the Warrant's sweeping breadth. The Warrant was not limited to a single search or seizure; nor was it limited to all three for a specific user. Rather, the Warrant authorized the FBI to repeatedly execute these searches and seizures—upwards of hundreds of thousands of times.

Warrant. However, the FBI instead logged the IP address of the transmission it received from the NIT, rather than determining the computer's assigned IP address. *See United States v. Matish*, No. 16-cr-16, 2016 WL 3545776, at *20 (E.D. Va. June 23, 2016).

1. The presence of government malware on a user's device is a Fourth Amendment seizure.

When the government sent malware to a user's computer, that malware exploited an otherwise unknown or obscure software vulnerability, turning the software against the user—and into a law enforcement investigative tool.

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). The presence of government malware on a user's computer (even if unnoticed by the user), and the manipulation of software running on that device, constitutes a Fourth Amendment seizure. *See* Report and Recommendation at 11-12, *United States v. Arterbury*, 15-cr-0018 (N.D. Ok. filed Apr. 25, 2016) (ECF No. 42).

Here, the targeted users undeniably have a possessory interest in their personal property—their computers and the private information stored on those computers. The government "interfere[d]" with that possessory interest when it surreptitiously placed code on the users' computers. Indeed, by exploiting a vulnerability in the software running on users' computers, the government exercised "dominion and control" over the exploited software. *Jacobsen,* 466 U.S. at 120-21 & n.18. 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 identification of Tor users. That exercise of "dominion and control," even if limited, constitutes a seizure. *Id.*; *cf Jones*, 132 S. Ct. at 949 (finding a Fourth Amendment search had occurred where "government physically occupied" individual's property by affixing a GPS tracker to it).

2. Operating malware on a user's computer is a Fourth Amendment search.

When the government's malware operated on the users' computers, that malware sought out certain information stored on the computers. This constitutes 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).

There can be no real dispute that individuals have a reasonable expectation of privacy in their computers and the private identifying information stored therein. As the Supreme Court recently 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 (citing *Boyd v. United States*, 116 U.S. 616, 630 (1886)). 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). It is no surprise, then, that courts uniformly recognize the need for a warrant prior to searching a computer. *See, e.g.*, *United States v. Payton*, 573 F.3d 859, 862 (9th Cir. 2009) ("Searches of computers . . . often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers."); *United States v. Andrus*, 483 F.3d 711, 718 (10th Cir. 2007) ("[C]omputers should fall into the same category as suitcases, footlockers, or other personal items that command[] a high degree of privacy.") (alteration in original) (internal quotation marks omitted), *reh'g denied*, 499 F.3d 1162 (10th Cir. 2007).

In this case, a search occurred because the government's malware operated directly on users' computers—a private area subject to a user's reasonable expectation of privacy. *Andrus*, 483 F.3d at 718. That is all that is required to give rise to a Fourth Amendment interest. *See Rakas v. Illinois*, 439 U.S. 128, 143 (1978) (Fourth Amendment protection depends on "a legitimate expectation of privacy in the invaded place"). The malware operated by "searching" the device's memory for the following information: "the type of operating system running on the

computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86)"; the computer's "Host Name"; the computer's "active operating system username"; and "media access control ("MAC") address." *See* Warrant at 2-3.[15]

In another case involving the same Warrant, a court in the Eastern District of Virginia mistakenly concluded in dicta that individuals lack a reasonable expectation of privacy in their computers because connecting them to the Internet "reduces" their ability to keep the contents private and leaves them vulnerable to outside hackers, such as the government in this case. *United States v. Matish*, No. 16-cr-16, 2016 WL 3545776, at *21-23 (E.D. Va. June 23, 2016). But, as the *Matish* court acknowledged, that conclusion directly contradicts precedent from a number of circuits, including its own. *Id.* at *21 (citing, *inter alia, Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001)).

If anything, individuals' increasing reliance on computers to store the "privacies of life" makes computers more deserving of Fourth Amendment protection, not less. *Riley,* 134 S. Ct. at 2494-95. Connecting a computer to the Internet does not perform a wholesale transformation and render private information on the computer accessible to the public. Nor does the occurrence of hacking over the Internet eliminate users' Fourth Amendment interests in their computers and the private information stored therein. Computers, like homes, may be vulnerable to forcible trespass. But just as the government implicates the Fourth Amendment if it enters people's homes, it does so too when it enters their computers. Here, it is undisputed that the government

[15] As noted above, EFF is not aware how, precisely, the malware operated on users' devices. Knowledge of those specifics could affect the analysis of the *invasiveness* of the search (*i.e.*, how much information the malware accessed and what specific areas of the computer were searched, etc.), but it does not alter the fact that a search occurred.

entered and seized the target computers in the course of deploying the NIT.[16] *See* Section I(A)(1), *supra.*

Other courts considering these cases have incorrectly reasoned that the search was constitutional because an individual has no reasonable expectation of privacy in an IP address. *See, e.g.*, *United States v. Werdene*, No. 15-cr-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016) (ECF No. 33); *Matish*, 2016 WL 3545776, at *20-21. Those decisions rely on *Smith v. Maryland*, 442 U.S. 735 (1979), and its related progeny, which involved warrantless access to information possessed *by a third party*. While some information obtained through this search might, in other contexts, be provided to or in the possession of a third party, that was not the case here. Rather, here, the government directly searched private areas on the user's computer. Hence, the so-called Third Party Doctrine has no applicability here precisely because this case "does not involve a third party." *United States v. Lambis*, No 15-cr-734, 2016 WL 3870940, at *7 (S.D.N.Y. July 12, 2016) (refusing to apply third party doctrine to government's collection of cell site information directly from defendant's phone). Instead, just as a search occurs if law enforcement physically enters a person's home and manually searches an individual's computer to locate information, so too does a search occur when the government employs technological means to achieve the same ends.

Thus, the relevant question in these cases is not whether the defendant had a reasonable

[16] The NIT makes use of a vulnerability on a target computer to deliver code, so it is not analogous to a police officer peering into a home through broken window blinds while standing in a public place. *See Matish*, at *23. Instead, deploying the NIT is more akin to an officer noticing a hidden defect in the lock on a home, opening the door, and conducting a search inside. *See, e.g., Kyllo v. United States,* 533 U.S. 27, 40 (2001) ("Where . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant.").

expectation of privacy in the information obtained through the search, but whether the defendant had a reasonable expectation of privacy *in the area where the search occurred*. *See Rakas*, 439 U.S. at 143. A search that occurs inside a person's home, on their personal computer, must be provided the Fourth Amendment's utmost protection.

3. Copying data from a computer is a Fourth Amendment seizure.

When the government's malware copied information from software running on users' computers, the copying of that data constituted a second seizure.

Again, a seizure occurs when the government "meaningful[ly] interfere[s]" with an individual's possessory interest in property. *Jacobsen,* 466 U.S. at 113. Courts recognize that individuals have possessory interests in information and that copying information interferes with that interest. *LeClair v. Hart*, 800 F.2d 692, 695, 696 n.5 (7th Cir. 1986) (recognizing it "is the information and not the paper and ink itself" that is actually seized). This is so because "the Fourth Amendment protects an individual's possessory interest in information itself, and not simply in the medium in which it exists." *United States v. Jefferson*, 571 F. Supp. 2d 696, 702 (E.D. Va. 2008); *United States v. Comprehensive Drug Testing, Inc.* ("*CDT*"), 621 F.3d 1162, 1168-71 (9th Cir. 2010) (referring to copying of data as a "seizure"); *Microsoft Corp. v. United States*, No. 14-2985, 2016 WL 3770056, at *17 (2d Cir. July 14, 2016) (same).

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

B. 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. The particularity requirement ensures that "those searches deemed necessary [are] *as limited as possible*."

Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971) (emphasis added). Particularity also prevents "[t]he issu[ance] of warrants on loose" or "vague" bases. Wayne R. LaFave, *Search and Seizure* § 4.6(a) (citing *Go-Bart Importing Co. v. United States*, 282 U.S. 344, 357 (1931)). The "uniformly applied rule is that a search conducted pursuant to a warrant that fails to conform to the particularity requirement of the Fourth Amendment is unconstitutional." *Massachusetts v. Sheppard*, 468 U.S. 981, 988 n.5 (1984).

As described above, each time the malware was deployed, a series of significant searches and seizures took place. Given the significance and invasiveness of those events, particularity was critical. But, for all the reasons that follow, the Warrant in this case failed to satisfy this elementary Fourth Amendment requirement.

1. The Government could have provided additional information in the Warrant—but chose not to.

The obstacles to investigation posed by Tor's privacy-enhancing technology do not justify use of a warrant authorizing a sweeping dragnet.

The particularity requirement is context-dependent, and the specificity required in a warrant will vary based on the amount of information available and the scope of the search to be executed. *United States v. Jones*, 54 F.3d 1285, 1291 (7th Cir. 1995); *see also United States v. Cardwell*, 680 F.2d 75, 78 (9th Cir. 1982). "[G]eneric classifications in a warrant are acceptable only when a more precise description is not possible." *United States v. Bright*, 630 F.2d 804, 812 (5th Cir. 1980). As the Seventh Circuit has explained, "courts have therefore demanded that . . . the warrant description must be *as particular* as circumstances permit." *United States v. Jones*, 54 F.3d at 1291 (quoting *United States v. Brown*, 832 F.2d 991, 996 (7th Cir. 1987)) (emphasis added).

Here, far more precision was not only possible but necessary. The FBI was in possession

of the server that hosted the site and had a clear window into the site's user activity. Based on this user 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 that was posted or accessed. Law enforcement could have done more still—such as reviewing site activity for evidence of a user's location or actual identity, or using the site's chat feature to engage individual users in conversations to learn more about their location or identity.

The inclusion of this information in the warrant application would have allowed the government to obtain a warrant based on *specific* facts, tied to *specific* users, thus authorizing searches and seizures against those specific, named users and their specific computers. *See Jones v. Wilhelm,* 425 F.3d 455, 462 (7th Cir. 2005) (warrant must satisfy particularity requirement at time of issuance and cannot leave particularity to "the discretion of police officers executing a warrant); *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986) (noting validity of warrant depends on "whether the government was able to describe the items more particularly in light of the information available to it at the time the warrant issued").

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

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

The Warrant here failed to meet the requirement of particularity in many ways.

Warrants require identification of a particular place to be searched and the particular person or thing to be seized. *Jones v. Wilhelm,* 425 F.3d at 462 (citing *Maryland v. Garrison,* 480 U.S. 79, 84 (1987)). For example, an arrest warrant for a specific individual is not sufficiently particularized to give officers the "authority to enter the homes of third parties" because it "specifies only the object of a search . . . and leaves to the unfettered discretion of the police the decision as to which particular homes should be searched." *Steagald v. United States*, 451 U.S. 204, 220 (1981). Any additional person or place to be searched requires a specific description in the warrant and an individualized showing of probable cause. *Greenstreet v. Cnty. of San Bernardino*, 41 F.3d 1306, 1309 (9th Cir. 1994); *United States v. Sims*, 553 F.3d 580, 582 (7th Cir. 2009); *see also Walter v. United States*, 447 U.S. 649, 656-57 (1980) ("[A] warrant to search for a stolen refrigerator would not authorize the opening of desk drawers.").

The Warrant here did not identify any particular person to search or seize. Nor did it identify any specific user of the targeted website. It did not even attempt to describe any series or group of particular users. Nor did it identify any particular device to be searched, or even a particular *type* of device. Instead, the Warrant broadly encompassed the computer of "*any* user or administrator" of the website. Warrant at 2 (emphasis added). Significantly, there were over 150,000 registered member accounts and over 1,500 daily visitors to the site. Aff. in Supp. of Warrant at 13, 18. The Warrant, on its face, thus authorized the search and seizure of as many as 150,000 individuals' computers and private information contained on those computers.

Compounding matters, the Warrant failed to provide any specificity about the place to be

searched—the location of the "activating computers."[17] Instead, the Warrant authorized the search of "any" activating computer, no matter where that computer might be located. Warrant at 2. Because an activating computer could be located anywhere in the world, the Warrant potentially authorized FBI searches and seizures in every U.S. state, every U.S. territory, and every country around the world.[18]

"Search 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); s*ee also Sims*, 553 F.3d at 582 (particularity requirement guards against "general, exploratory rummaging"). Such is the case here: the government obtained a single warrant, authorizing the search of over 150,000 users located all over the world, the definition of a "virtual, all-encompassing dragnet" prohibited by the Fourth Amendment.

3. The Warrant vested too much discretion in the executing officers.

The Fourth Amendment's particularity requirement makes general searches "impossible" by ensuring that, when it comes to what can be searched or seized, "nothing is left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927); *see also Stanford,* 379 U.S. at 481 (particularity helps eliminate the threat of "officers

[17] The Warrant listed the Eastern District of Virginia as the location of the property to be searched. As described *supra*, that was incorrect: the searches occurred on users' computers, wherever they were located. EFF does not address the legal consequences of that error for the purposes of Federal Rule of Criminal Procedure 41 in this brief.

[18] Indeed, it appears that the government did conduct overseas searches based on the Warrant. Joseph Cox, *New Case Suggests the FBI Shared Data from Its Mass Hacking Campaign with the UK*, Motherboard (Feb. 10, 2016), *available at* https://motherboard.vice.com/read/new-case-suggests-the-fbi-shared-data-from-its-mass-hacking-campaign-with-the-uk. The government's decision to conduct these searches—and the magistrate's decision to authorize them—raises special considerations when the searches can take place worldwide. *See Microsoft Corp.*, 2016 WL 3770056, at *11 (noting that Fourth Amendment traditionally limits warrants to domestic investigations).

acting under the unbridled authority of a general warrant").

As a result of its overbreadth in authorizing the search of "any" activating computer, the Warrant gave executing officers vast discretion to decide who to target and how to accomplish the searches and seizures. It granted the FBI carte blanche to define: how the malware would be deployed and how it would operate; what portions of the activating computers the malware would search; and which of the hundreds of thousands of users it would be deployed against—limits that the Fourth Amendment requires be imposed by a neutral and detached magistrate.

In fact, the warrant application explicitly *sought* such free rein. As the government explained, "in order to ensure technical feasibility and avoid detection of the technique by subjects of investigation, the FBI would deploy the technique more discretely against particular users." Aff. in Supp. of Warrant at 12 n.8. In other words, the government deployed different types of malware (or the same malware, in different ways) against different users. The government thus conducted its searches and seizures in different ways against different users—all at the investigating officer's discretion.

Notably absent from the Warrant was any meaningful limitation on the operation of the malware. Given that the malware carried out a search of a user's private computer, *see supra* at 9, this type of tailoring was particularly critical. *See CDT*, 621 F.3d at 1168-71; *United States v. Mann*, 592 F.3d 779, 782, 785–86 (7th Cir. 2010).

Ultimately, and despite its facial appeal, the FBI's request to act with a free hand is in fact further evidence of the constitutional violation. *See Groh v. Ramirez*, 540 U.S. 551, 560-61 (2004) ("Even though petitioner acted with restraint in conducting the search, the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer.") (citing *Katz*, 389 U.S. at 356). Warrants, and the particularity requirement specifically, are designed so

that the searches authorized are "as limited as possible." *Coolidge*, 403 U.S. at 467. That was not the case here: the government cast its net as widely as possible giving agents discretion over who it would target and in what manner. But leaving the operation of a dragnet to the "discretion of the State" is "fundamentally offensive to the underlying principles of the Fourth Amendment." *Bridges*, 344 F.3d at 1016.

4. The Warrant exceeds even other constitutionally suspect warrants, including roving wiretaps, "all persons" warrants, and anticipatory warrants.

In limited but factually distinct circumstances, courts have sanctioned warrants that rely on expansive interpretations of the Fourth Amendment's particularity requirement. While the Warrant in this case bears some passing resemblance to these types of warrants—roving wiretaps, so-called "all persons" warrants, and anticipatory warrants—none are as general as the Warrant in this case.

Roving wiretaps 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).[19] 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. *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 (9th

[19] In contrast, 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*, 388 U.S. at 56, 59.

Cir. 1992).[20] Here, by contrast, no specific suspect 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 framework, one that imposes additional safeguards, in the face of constitutional uncertainty. Instead, the government made up rules—broad ones—as it went along.

"All persons" warrants are another unusual—and indeed constitutionally suspect—type of warrant that nevertheless contain greater particularity than the Warrant issued here. These warrants authorize the search of a particular place, as well as "all persons" on the premises at the time the search is conducted. *See Marks v. Clarke*, 102 F.3d 1012, 1029 (9th Cir. 1996). As a threshold matter, the constitutionality of these warrants is "far from settled law." *Mongham v. Soronen*, 2013 WL 705390, at *6 (S.D. Ala. Feb. 26, 2013); *see also Ybarra v. Illinois*, 444 U.S. 85, 92 n.4 (1979) ("Consequently, we need not consider situations where the warrant itself authorizes the search of unnamed persons in a place[.]"). Indeed, some courts have concluded that "all persons" warrants are *per se* unconstitutional. *See United States v. Guadarrama*, 128 F. Supp. 2d 1202, 1207 (E.D. Wis. 2001) (collecting cases and noting "the minority view, held or suggested by eight jurisdictions, is that 'all persons' warrants are facially unconstitutional because of their resemblance to general warrants").

Even assuming its constitutionality, EFF is not aware of an "all persons" warrant that comes close to approximating the scope and reach of the Warrant at issue here. First, "all persons" warrants are by definition tied to the search of a particular physical location—something the Warrant here conspicuously lacked. Second, "all persons" warrants are necessarily limited in scope by physical constraints. These warrants have generally authorized the search of a small

[20] 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.

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 the search of over a hundred thousand users' devices around the world. *See Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (noting electronic surveillance evades "ordinary checks" on abuse).

The Warrant here was in fact yet another species of constitutionally problematic warrant—an anticipatory warrant. An anticipatory warrant is one based on "probable cause that at some future time (but not presently) certain evidence of a crime will be located at a *specified place*," 2 LaFave, Search and Seizure § 3.7(c), p. 398 (4th ed. 2004) (emphasis added). Although they are not "categorically unconstitutional," *United States v. Grubbs*, 547 U.S. 90, 94 (2006), these warrants, when 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." *Id*. at 96. 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*. The Warrant here was unquestionably an anticipatory one. The search and seizure of an "activating computer" was predicated on a user logging into Playpen in the future. *See* Warrant at 2. Underscoring the particularity problems here, the affidavit failed to describe a "likelihood that the condition w[ould] occur"—that a user would log into the website—tied any *specified* one of the 150,000 users of the site (or, for that matter, for any future registered user of the site). The Warrant thus more closely resembles the anticipatory warrant for "every house in the country, authorizing search and seizure *if*" the predicated event occurs—not a particularized authorization to search specific places.

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, like the Warrant did here.

II. Complying with the Fourth Amendment Does Not Create an Insurmountable Bar for Law Enforcement, Even in Cases Like This.

To be clear, requiring greater particularity in circumstances like this will not insulate Tor users engaging in criminal activity from prosecution. Nor will it deprive the FBI of a valuable law enforcement tool or otherwise "fr[eeze] into constitutional law [only] those law enforcement practices that existed at the time of the Fourth Amendment's passage." *Payton v. New York,* 445 U.S. 573, 591 n.33 (1980).

As described above, the government could and should have provided a more specifically tailored application and narrowed the Warrant's scope dramatically by specifying the user or users against whom it wanted to deploy its malware, based on particular showings of probable cause.

But law enforcement cannot rely on new surveillance techniques "blindly." *Arizona v. Evans*, 514 U.S. 1, 17-18 (1995) (O'Connor, J., concurring). "With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities." *Id*. With appropriate tailoring and sufficient specificity, a valid warrant could issue for the deployment of malware, even under the circumstances present here. But, in this case, the government consciously chose to cast its net as broadly as possible, neglecting those constitutional responsibilities.

CONCLUSION

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

DATED: August 3, 2016 *<u>/s/ Christopher Donovan</u>*

Christopher Donovan
PRUHS & DONOVAN, S.C.
757 N. Broadway, Suite 401
Milwaukee, Wisconsin 53202
Phone: (414) 221-1950
Fax: (414) 221-1959
donovanc34@hotmail.com

Mark Rumold
Andrew Crocker
Stephanie Lacambra
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Attorneys for Amicus Curiae Electronic Frontier Foundation

CERTIFICATE OF SERVICE

I hereby certify that on this 3rd day of August, 2016, I caused copies of the foregoing Brief of *Amicus Curiae*, Electronic Frontier Foundation, to be served by electronic means via the Court's CM/ECF system on all counsel registered to receive electronic notices.

/s/ Christopher Donovan