HONORABLE MARSHA J. PECHMAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. BRUCE LORENTE, Defendant.	No.: CR15-0274MJP **BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION** **NOTE ON MOTION CALENDAR:** March 18, 2016

focal PLLC
900 1st Avenue S., Suite 203
Seattle, WA 98134
206.529.4827

TABLE OF CONTENTS

focal PLLC
900 1st Avenue S., Suite 203
Seattle, WA 98134
206.529.4827

TABLE OF AUTHORITIES

CASES

focal PLLC
900 1st Avenue S., Suite 203
Seattle, WA 98134
206.529.4827

focal PLLC
900 1st Avenue S., Suite 203
Seattle, WA 98134
206.529.4827

STATUTES

OTHER AUTHORITIES

focal PLLC
900 1st Avenue S., Suite 203
Seattle, WA 98134
206.529.4827

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 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; journalists use Tor; attorneys use Tor; corporations use Tor; and governments use Tor.

It is undisputed that criminals can also use Tor's privacy-enhancing technologies. But law enforcement attempts to subvert Tor users' privacy 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 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

focal PLLC
900 1st Avenue S., Suite 203
Seattle, WA 98134
206.529.4827

facts, alone, are sufficient to render the warrant invalid.

And be sure: the use of Tor did not require the government to seek a warrant as sweeping as the one they 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 users, and their 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. Nevertheless, the government sought—and received—authorization to cast its electronic net as broadly as possible.

But the breadth of that net ran afoul of the Fourth Amendment's requirements. "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 481-82.

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, 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-

[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

focal PLLC
900 1st Avenue S., Suite 203
Seattle, WA 98134
206.529.4827

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 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 visitor's location.

II. Malware and Government 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]

---

[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.

[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.

focal PLLC
900 1st Avenue S., Suite 203
Seattle, WA 98134
206.529.4827

Relevant here is a specific type of malware known as a Remote Administration Tool (or "RAT," also referred to as a Remote Access Tool or Remote Access Trojan).[10] RATs operate 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] Capabilities of a RAT often include "keystroke logging, file system access and remote control, including control of devices such as microphones and webcams."[12] Hackers use RATs to extract sensitive information, such as financial information, photos, and personal communications, from a computer.[13]

The government calls the RATs it uses during investigations a Network Investigative Technique ("NIT"). *See* Resp. to Def.'s Mot. to Suppress at 5, *United States v. Michaud*, No. 15-cr-05351, ECF No. 140 (W.D. Wash. Jan 28, 2016) (ECF No. 47) ("*Michaud* Government Response"). The government has strongly 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. In the government's view, *its* use of this type of software is not malicious because it is "authorized," in the sense that a court sanctioned its use. *Id.* However, there is no technical distinction between the "NITs" used by the government and the "RATs" used by hackers. For clarity, we refer to this type of software only as "malware" in the balance of the brief.

III. Law Enforcement's Investigation of Play Pen

EFF understands that this case arises from the same set of facts as *United States v. Michaud*, No. 15-cr-05351, ECF No. 140 (W.D. Wash. Jan 28, 2016), which describes a law

[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] Context, *Malware Analysis - Dark Comet RAT* (Nov. 2, 2011), http://www.contextis.com/resources/blog/malware-analysis-dark-comet-rat/.

[12] *Id*.

[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.

focal PLLC
900 1st Avenue S., Suite 203
Seattle, WA 98134
206.529.4827

enforcement investigation of Play Pen, 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"). *See* Suppression Order at 3-4, *Michaud*, ECF No. 140 ("*Michaud* Order"). While some of the details of the technology involved remain under seal or have not been disclosed by the government, enough information is in the public record to understand generally how the investigation proceeded.

According to the government, it took physical possession of the server or servers that hosted Play Pen and assumed the role of website administrator for a two-week period. *Michaud* Government Response at 5. 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.* at 5-7.

Play Pen operated as a Tor hidden service. *Id.* at 4; *see also Lorente* Compl. ¶¶ 3-7. As noted above, in its normal mode of operation, the operators of a Tor hidden service do not have access to the identifying details—such as the IP addresses—of visitors to the site. *Id*. In the course of its investigation, during the period while the government was operating Play Pen, investigators used malware to infect the computers of users who logged into the site. *Michaud* Government Response at 5-6. 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 at least two different kinds of malware were served to different types of users of the site. *Id.* at 5-6 n.6. From the publicly available information, it appears that for some target users, "such as those who attained higher status on the website," the government deployed a more sophisticated version of the malware—one that used a different, less detectable vulnerability to infect users' computers.

But the operation of the two types of malware was similar: code served by the government to the target computers used one or more vulnerabilities in the users' software in order to search and extract identifying data (IP addresses and other related information) that the

focal PLLC
900 1st Avenue S., Suite 203
Seattle, WA 98134
206.529.4827

Tor network would otherwise have made unavailable.

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 terms of both breadth and the discretion it provided to the officials executing it. That breadth is underscored by the significance of the activities it authorized the FBI to perform: infecting an individual's software and computer, 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 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 *every time* the government deployed its malware. Each use caused three Fourth Amendment events to occur: (1) a 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.

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

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

focal PLLC
900 1st Avenue S., Suite 203
Seattle, WA 98134
206.529.4827

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.

Here, the targeted users undeniably have a possessory interest in their personal property—their computers and the software operating 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 United States v. Jones*, 132 S. Ct. 945, 949 (2012) (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 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

focal PLLC
900 1st Avenue S., Suite 203
Seattle, WA 98134
206.529.4827

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").[14] The malware operated by "searching" the device's memory for the following information: the computer's IP address; "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 Michaud* Suppression Order at 4-5.[15] Just as a search would have occurred if a law enforcement officer manually reviewed an individual's computer to locate this information, so too did a search occur when the government employed technological means to reach the same ends.

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

When the government's malware copied information from software running on the users'

[14] While some of the information obtained in the search might, in other contexts, be provided to third parties, the government did not obtain the information here from any third party. Rather, it directly searched private areas on the user's computer. Hence, the so-called Third Party Doctrine, *see Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) has no applicability here. *See Rakas*, 439 U.S. at 143.

[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.

focal PLLC
900 1st Avenue S., Suite 203
Seattle, WA 98134
206.529.4827

computers, the copying of that data constituted a second seizure.

Again, a seizure occurs when the government "meaningfully 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) (quoting *Jacobsen*, 466 U.S. at 113) (recognizing it "is the information and not the paper and ink itself" that is actually seized).

"[W]hile copying the contents of a person's documents . . . does not interfere with a person's possession of those documents, it does interfere with the person's *sole* possession of the information contained in those documents[.]" *United States v. Jefferson*, 571 F. Supp. 2d 696, 703 (E.D. Va. 2008) (emphasis added). This is because "the Fourth Amendment protects an individual's possessory interest in information itself, and not simply in the medium in which it exists." *Id*. at 702; *see also 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"); *United States v. Ganias*, 755 F.3d 125, 137 (2d Cir. 2014), *reh'g en banc granted,* 791 F.3d 290 (2d Cir. 2015).

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 (1931)).

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 this elementary Fourth Amendment requirement.

focal PLLC
900 1st Avenue S., Suite 203
Seattle, WA 98134
206.529.4827

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 did not justify a warrant as sweeping as the one obtained.

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. *See United States v. Cardwell*, 680 F.2d 75, 78 (9th Cir. 1982) (noting that in assessing the validity of warrants, "[o]ne of the crucial factors to be considered is the information available to the government"); *Maryland v. Garrison*, 480 U.S. 79, 85-86 (1987) (officers who know they do not have probable cause to search a place are "plainly" obligated to exclude it from a warrant request).

Because the FBI was in possession of the server that hosted the site, the government 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 users' 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.

These additional investigative steps would have allowed the government to obtain a warrant based on *specific* facts, tied to *specific* users, and thus authorizing searches and seizures against those specific, named users and their specific computers. *See 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 have still been unknown, the warrant would have at least begun to target specific individuals based on specific probable cause determinations. *See Cardwell*, 680 F.2d at 78 ("Generic classification in a

focal PLLC
900 1st Avenue S., Suite 203
Seattle, WA 98134
206.529.4827

warrant are acceptable only when a more precise description *is not possible*.") (emphasis added) (quoting *United States v. Bright*, 630 F.2d 804, 812 (5th Cir. 1980).

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

The Warrant here failed the to meet the familiar (and necessary) requirements of particularity in myriad ways.

Warrants require identification of a particular individual and the particular place to be searched. *See Maryland v. King*, 133 S. Ct. 1958, 1980 (2013) (warrant lacks particularity if "not grounded upon a sworn oath of a specific infraction by a *particular individual*, and thus not limited in scope and application"). 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. *See Greenstreet v. Cnty. of San Bernardino*, 41 F.3d 1306, 1309 (9th Cir. 1994); *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 name any specific person. 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. Similarly, it did not identify any particular device to be searched, or even a particular *type* of device. Instead, the Warrant broadly encompassed the computer of "*any* user or administrator" of the website. *Michaud* Order at 4 (emphasis added). Significantly, there were "200,000 registered member accounts and 1,500 daily visitors" to the site. *Id.* at 2. The Warrant, on its face, thus authorized the searches and seizures described above for as many as 200,000 individuals' computers.

Compounding matters, the Warrant failed to provide any specificity about where the

focal PLLC
900 1st Avenue S., Suite 203
Seattle, WA 98134
206.529.4827

searches would be carried out—the location of the "activating computers."[16] Instead, the Warrant authorized the search of "any" activating computer, no matter where that computer might be located. *Id.* at 4. Because an activating computer could conceivably be located anywhere in the world, the Warrant conceivably authorized FBI searches and seizures in all 50 U.S. states, every U.S. territory, and every country around the world.[17]

"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). Such is the case here: the government obtained a single warrant, authorizing the search of upwards of 200,000 users located around the world. That is far closer to a "virtual, all-encompassing dragnet" than a specific, particularized warrant required 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 acting under the unbridled authority of a general warrant").

As a result of its breadth, authorizing the search of "any" activating computer, the Warrant gave executing officers total discretion to decide which users to target and the manner in which to accomplish the searches and seizures. It thus left to the FBI to decide: how the malware

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

[17] 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.

focal PLLC
900 1st Avenue S., Suite 203
Seattle, WA 98134
206.529.4827

would be deployed; how the malware operated; what portions of the activating computers the malware would search; and which of the hundreds of thousands of users of the site it would be deployed against.

In fact, the warrant application explicitly *sought* that discretion. 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." *Michaud* Government Response at 5 n.6. Thus, the government deployed different types of malware (or the same malware, in different ways) against different users. Thus, the government conducted its searches and seizures in different ways against different users—all at the investigating officer's discretion.

Particularly absent from the Warrant was some, meaningful limitation on the operation of the malware. Given that the malware effectuated a search of user's private computer, *see supra* at 9, this type of tailoring was particularly critical. *See CDT*, 621 F.3d at 1168-71.

Despite its facial appeal, the FBI's request to act at its discretion 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 and, at its own election, decided 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. Other types of warrants that push the boundaries of the Fourth Amendment's particularity requirement are still more narrow and specific than the Warrant here.

In limited but factually distinct circumstances, courts have sanctioned warrants that rely

focal PLLC
900 1st Avenue S., Suite 203
Seattle, WA 98134
206.529.4827

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 and so-called "all persons" warrants—neither type is 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 suspect will use. *See United States v. Petti*, 973 F. 2d 1441, 1444-46 (9th Cir. 1992).[18] 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 Cir. 1992).[19] 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. 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

[18] In contrast, in an application for a fixed wiretap, "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.

[19] 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.

focal PLLC
900 1st Avenue S., Suite 203
Seattle, WA 98134
206.529.4827

that "all persons" warrants are *per se* unconstitutional. *See United States v. Guadarrama*, 128 F. Supp. 2d 1202, 1207 (E.D. Wis. 2001) (collecting cases and noting "the minority view, held or suggested by eight jurisdictions, is that 'all persons' warrants are facially unconstitutional because of their resemblance to general warrants").

Even assuming their constitutionality, 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, known place—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 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 upwards of 200,000 users' devices across the world. *See Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (noting electronic surveillance evades "ordinary checks" on abuse).

In sum, roving wiretaps authorize surveillance of *specific* people using unnamed facilities, while "all persons" warrants authorize the search of unnamed people in *specific* places. But no constitutional warrant can authorize the search of unnamed (and unlimited) persons in unnamed (and unlimited) places, like the Warrant did here.

II. Requiring Compliance 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 these 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 have provided a more specifically tailored application and narrowed the Warrant's scope dramatically. That approach could have allowed

focal PLLC
900 1st Avenue S., Suite 203
Seattle, WA 98134
206.529.4827

the government to deploy its malware, in a targeted fashion, against particular individuals 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 its constitutional responsibilities.

DATED: February 26, 2016

/s/ Venkat Balasubramani

Venkat Balasubramani, WSBA #28269
FOCAL PLLC
900 1st Avenue S., Suite 203
Seattle, WA 98134
Telephone: (206) 529-4827
Facsimile: (206) 260-3966
venkat@focallaw.com

Mark Rumold
Nate Cardozo
Andrew Crocker
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 26th day of February, 2016 I caused copies of the foregoing Brief of *Amici 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/ Venkat Balasubramani
Venkat Balasubramani

focal PLLC
900 1st Avenue S., Suite 203
Seattle, WA 98134
206.529.4827