JUDGE \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

AT SEATTLE

|  |  |  |
| --- | --- | --- |
| UNITED STATES OF AMERICA,  Plaintiff,  v.  John DOe,  Defendant. | )  )  )  )  )  )  )  )  )  ) | No. CR15-  MOTION AND MEMORANDUM IN SUPPORT OF MOTION TO SUPPRESS EVIDENCE  ***[Evidentiary Hearing Requested]***  **FILED UNDER SEAL**  **Noted: March 4, 2016** |

**I. INTRODUCTION**

John Doe, through his counsel Colin Fieman and Mohammad Hamoudi, respectfully moves the Court pursuant to Fed. R. Crim. P. 12(b)(3)(c) for an order suppressing all evidence seized from Mr. Doe’s home computer by the FBI on or about February 24, 2015. The evidence, consisting of an “internet protocol” (IP) address and other electronic data, was seized by the Government with a “Network Investigative Technique” (NIT), a type of malware that was secretly inserted by FBI agents located in Virginia onto Mr. Doe’s computer in Seattle, Washington.

The NIT altered and overrode security settings on the computer; allowed the FBI to remotely search for and collect data from the computer’s hard drive; and then transmitted that data to FBI agents in Virginia. Mr. Doe also seeks suppression of all fruits of this illegal search, including any allegedly inculpatory statements by him.

While the search and seizure technology involved in this case is sophisticated, the key facts are undisputed and the applicable legal principles are well established. Mr. Doe raises five specific grounds for suppression.

**First**, the remote search of Mr. Doe’s home computer was undertaken pursuant to a warrant that is not supported by probable cause. As set forth below, the Government sought authorization to search the computers of everyone who visited the home (or “log in”) page of a web site called “Playpen.” *See* exhs. A and B (the NIT warrant and supporting application). Probable cause for these searches turned on whether it “unabashedly announced” that it was a child pornography site. Playpen had a mix of legal and illegal content, as well as chat and message forums, and it did not advertise itself as a child pornography site. *See* exh. C (Playpen’s home page).

The lack of facts in support of probable cause is made even more problematic because, according to the Government, the warrant authorized 100,000 or more searches anywhere in the world. As a result, the scope of the search and seizure authority the Government is claiming in this case is unprecedented.[[1]](#footnote-1)

**Second**, the FBI intentionally or recklessly misled the issuing court about how the site appeared, among other false and misleading statements. Specifically, the warrant application alleged that the site’s home page displayed purportedly lascivious pictures that advertised illegal content on the site. In truth, the FBI had seized control of the site before applying for the warrant and knew that these pictures had been removed. The defense therefore requests a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978).

**Third**, the NIT warrant was an anticipatory warrant and the “triggering event” that would establish probable cause for searches did not occur. As set forth in the warrant application, the triggering event was the act of visiting Playpen’s home page as it was described in the application and then electing to enter the site. However, the triggering event did not occur in this case because the FBI had included a false description of the home page in the application. The home page as it actually appeared at the time the warrant was issued and the searches were executed did not, as the FBI had claimed, show that the site contained child pornography. The search in this case therefore exceeded the scope of the warrant’s authorization, the “good faith” exception is inapplicable, and suppression is required.

**Fourth**, the NIT warrant was issued in the Eastern District of Virginia (EDVA) and it only authorized searches of persons or property located in that district. Consequently, the search of Mr. Doe’s Washington computer exceeded the scope of the EDVA warrant. Further, the “good faith” exception to the exclusionary rule does not apply when a search is executed in a location that is not authorized by the underlying warrant.

**Fifth,** if the NIT warrant had authorized searches outside the district in which it was issued (as the Government will claim it does), then the warrant would have violated Fed. R. Crim. P. 41. According to the Government, the warrant authorized the FBI to search computers anywhere in the world. But this argument makes no sense because it not only disregards the jurisdictional limitations of Rule 41, it assumes that the Magistrate Judge who issued the warrant knowingly violated the Rule and 18 U.S.C. § 3103. Moreover, even if the issuing judge had erred and the warrant could be construed as authorizing searches anywhere, Ninth Circuit precedents require the suppression of evidence that is seized in violation of Rule 41’s jurisdictional limitations.

Finally, in conjunction with this motion, Mr. Doe is filing a separate Motion to Dismiss Indictment based on outrageous governmental conduct. The Government executed all of its NIT searches, including the search of Mr. Doe’s computer, after the FBI had seized control of Playpen on February 19, 2015. Between February 20, 2015, and March 4, 2015, the FBI did not simply monitor the site and identify visitors, but instead published and distributed massive amounts of child pornography from various sub-forums within it. This aspect of the investigation was not disclosed to the judge who issued the NIT warrant and was illegal, since there are no statutory or other legal exemptions that allow law enforcement to publicly disseminate child pornography.

The FBI’s actions were also grossly irresponsible because there was no investigatory need for agents to distribute child pornography in order to identify the people who were visiting Playpen and accomplish the FBI’s investigatory goals.

As a result, the Government has done far more to re-victimize the children depicted in the pictures that were distributed from Playpen than have any of individual defendants in this district who are alleged to have downloaded pornography from the site. Even if the Court determines that dismissal is too exceptional a remedy for the Government’s conduct, suppression is an appropriate alternative.

In short, this case presents novel and important issues involving the Fourth Amendment and privacy rights in an increasingly Internet-driven world, governmental adherence to the rule of law, and the Government’s duty of candor to the courts. Any one of the grounds set forth in this motion warrants suppression. When the Court considers the totality of the circumstances, suppression is not only appropriate but necessary to deter future overreaching by the Government.

# II. Statement of Facts

**A. The Playpen Web Site and the Tor Network**

On July 28, 2015, law enforcement agents executed a search warrant at the home of John Doe in Seattle*,* Washington, and physically seized (among other items) several personal computers. This search was the second search of Mr. Doe’s home, the first having occurred on or about February 24, 2015, when the FBI used a “Network Investigative Technique” (NIT) malware to conduct a remote search of the contents of one of Mr. Doe’s personal computers. It is this initial February, 2015, data search that is the focus of Mr. Doe’s Fourth Amendment challenges.

According to the discovery, the events leading to the two searches of Mr. Doe’s home began in December, 2014, when a “foreign law enforcement agency” happened upon the website Playpen, learned that it contained child pornography, and alerted the FBI.

Playpen operated on a network commonly known as “the onion router” or “Tor” network. Tor was created by the U.S. Naval Research Laboratory and it is primarily funded by the U.S. Government. The network is designed to “protect user privacy online.” Exh. B (the NIT warrant application) at ¶ 8. In simple terms, people who want to use the Tor network can download a free browser and search engine (similar to Chrome or other Internet browsers) that provides added privacy protections. *See* <https://www.torproject.org> (“Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security”). Activities and communications on Tor (like visiting a website) are routed through multiple computers (or “nodes”) to protect the confidentiality of the Internet Protocol (IP) addresses and other identifying information of its users. *See* exh. B at ¶¶ 6-9. Using the Tor network is comparable to having the Internet equivalent of an unlisted phone number and caller I.D. blocking.

Like the Internet in general, the Tor network can be used for both legitimate and illicit purposes. *See* James Ball, *Guardian Launches Secure Drop System for Whistleblowers to Share Files*, The Guardian, June 5, 2014 (describing the newspaper’s use of Tor as a secure means for communicating with whistleblowers);[[2]](#footnote-2) Virginia Hefferman, *Granting Anonymity*, N.Y. Times, December 17, 2010 (“Peaceniks and human rights groups use Tor, as do journalists, private citizens and the military, and the heterogeneity and farflungness of its users – together with its elegant source code – keep it unbreachable.”).[[3]](#footnote-3) Millions of people now routinely use the Tor network to avoid being targeted by advertising, to protect their personal data from marketing companies and scammers, and to search for a wide variety of content that they wish to keep private.

In this case, due to an error in Playpen’s connections with the Tor network, it could be found and viewed on both the Tor network and the regular Internet for at least part of the time that it was operating. The FBI was able to locate the operator of the site and raided his home in Naples, Florida, on February 19, 2015.

**B. The FBI’s Distribution of Pornography From Playpen**

The same day, the FBI took control of Playpen and moved its server to a government facility in Virginia, where it maintained and operated the site at least until March 4, 2015.[[4]](#footnote-4) During this time the FBI continued to operate the site as an active distributor of child pornography and took no measures to block or limit the uploading, downloading or redistribution of thousands of illicit pictures and videos.

As of February 20, the site had 158,094 members from all over the world. Exh. B at ¶ 11. According to the discovery, it appears that approximately 56,000 new members joined the site after the FBI took it over and approximately 100,000 people visited the site during the two week period that the FBI was operating it. This was a dramatic increase over the approximately 11,000 weekly visitors the site had before the FBI took it over. *See* Exh. B at ¶ 19.

**C. The Virginia “Network Investigative Technique” Warrant**

On February 20, 2015, the Government submitted its application for the NIT warrant to Magistrate Judge Theresa Carroll Buchanan of the Eastern District of Virginia. In the application, the affiant states that “the entirety” of Playpen is “dedicated to child pornography,” exh. B. at ¶ 27, and also describes the site as a “website whose primary purpose is the advertisement and distribution of child pornography.” Exh. B at ¶ 11. More accurately, Playpen offered a mix of chat forums, private messaging services, both legal and illegal pictures and videos, and links to pictures and videos. *See* exh. D (Playpen’s table of contents); exh. B at ¶ 14.[[5]](#footnote-5)

The warrant application sought authorization to use a “Network Investigative Technique” to search “activating computers,” which were defined as the computers “of any user or administrator who logs into the TARGET WEBSITE by entering a username or password.” Exh. A at Bates 375 (“Attachment A”). The username and password could be made up and entered on the spot (there was no verification or other steps required to enter the site), and the site was free.

Somewhat confusingly, the actual targets of the NIT warrant were the “activating computers,” not the “TARGET WEBSITE,” which refers to Playpen. Not only had the FBI already seized Playpen, its server and records did not contain any of the visitor data the FBI wanted to search for pursuant to the warrant. Nor could that data be collected from third parties, such as Comcast or other Internet service providers, since the basic purpose of the Tor browser and network is to privatize its users identities and activities. Exh. B at ¶¶ 8-9, 29.

Accordingly, the warrant application explains that the FBI would use its NIT to search for data directly on the personal computers and other digital devices of anyone who visited the Playpen site. This data included user addresses; the type of operating systems on their computers; and various other data that would not otherwise be disclosed by a computer’s owner or user. *Id*. at Bates 376 (“Attachment B”). Elsewhere in the application, the NIT is broadly described as hidden “computer instructions,” or code, that agents would send to the unidentified targets when they landed on the home page and typed in a name or password. *Id.* at ¶ 33. Since this code was “hidden” visitors to the site had no knowledge that their computers were infected with it when they visited Playpen. And, because the NITs gained access to personal computers without the owner or user’s knowledge or consent, the NIT is a form of “malware.” *See* exh. F at 117 (Testimony of Dr. Christopher Soghoian).

Once the FBI had inserted a NIT onto a computer, it did several things to execute a search on and seize data from that computer. First, the NIT altered or overrode a computer’s security settings to install itself on the targeted computer, similar to disabling a home’s burglar alarm system before climbing through a window. *Id*. at 113-118.

Next, the NIT searched the computer’s hard drive and operating system for the data that the FBI wanted. *See id*. This is the technical equivalent of searching desks or file cabinets in the house to find an address book or billing records that contain the information the FBI was looking for. In this case, Mr. Doe’s computer was located in his home when it was remotely searched by the FBI and he had no knowledge that the search had even occurred until it was disclosed by the Government on September 14, 2015 (almost seven months after the fact).

Finally, the NIT overrode the user’s Tor browser protections and forced the computer to send the seized data back to the FBI, where it was stored in the digital equivalent of an evidence room on a government server. *Id*. at 115-116.

As many as 100,000 people visited Playpen while it was under FBI control. The Government maintains that all of those visitors were authorized targets of the NIT searches, and it is unclear at this point how many of the 100,000 potential targets were actually subjected to data searches.

Playpen had a mix of legal and illegal content, as well as chat forums, and the NIT warrant application does not allege that everyone who visited the site necessarily viewed illegal pictures. The warrant application nevertheless sought authorization to search the computers of anyone who simply passed through the home page. The affiant therefore focused on the appearance and contents of the home page to establish probable cause to believe that anyone accessing the site was committing a crime. In this regard, the application describes the home page as containing a banner with “two images depicting partially clothed prepubescent girls with their legs spread apart.” Exh. B at ¶ 12. The application did not claim that these pictures meet the legal definition of “lascivious” pornography, in 18 U.S.C. § 2256(2)(A), and the application did not include a copy of the home page.

Moreover, the description of the home page is inaccurate. In October, 2015, the defense requested a “screen shot” (printed copy) of the site’s home page as it appeared between February 20 and March 4 (the time during which the FBI was operating the site and searching computers). On November 10, 2015, the Government turned over a copy of the home page that included the suggestive images that were described in the NIT warrant application. However, on closer inspection, the defense learned that the screen shot had been taken on February 3, 2015 (17 days prior to the warrant application). It was only after the defense renewed its demand for the relevant screen shot that the FBI disclosed it. *See* exh. C. The home page, as it actually appeared from February 19 (the day before the warrant application) until the site was shut down, is devoid of any highly sexualized images of prepubescent girls, and instead shows a picture of a fully clothed female, legs crossed. While the girl depicted on the home page appears to be young, the image is small and it is not clear that she is under the age of 18, let alone “prepubescent.”

Further, discovery related to the February 19 search of the original site operator’s Florida home confirms that the FBI was aware of the site’s actual appearance on that date. Nevertheless, the FBI did not disclose this information in the warrant application presented to Magistrate Judge Buchanan the following day, and it never submitted an amended or corrected affidavit.[[6]](#footnote-6)

The warrant application goes on to describe text on the home page that advises visitors not to “copy and paste” and states “No Cross-Board Posts, .7Z preferred, Encrypt File Names, Include Preview,” along with a place to login or register as a new user. *See* exh. B at ¶ 12. The affiant did not claim that the technical text is indicative of criminality and explained, *inter alia*, that terms like “‘no cross-board reposts’ refers to a rule against posting material that had been posted on other websites. *Id*.

The rest of the material about the site describes child pornography that could be found in various sub-directories. After signing in to Playpen, visitors were directed to a “table of contents” listing 46 different forums and sub-directories. Exh. B at ¶ 27;exh. D (the table of contents). Like the home page, the table of contents did not contain child pornography (the graphics on the page depict onions, a visual reference to the Tor network) and it listed a variety of topics. Most of these clearly relate to sexual matters or fetishes, and some of these also clearly relate to children. Other than the reference to “HC” (according to the affiant, standing for “hard core”) on four of the forums, it is not obvious that they contain child pornography. Some of the content consisted of written “stories,” legal child “erotica,” and a variety of other forums with names like “general discussion” and “artwork.” *See* exh. B at ¶¶ 5(b) & 14; exh. D.

The table of contents, moreover, could be viewed only *after* someone had logged in to the site, at which point the FBI had already remotely searched the visitor’s computer. From there, in order to locate pictures or videos, a visitor would have to take the additional steps of selecting one of the sub-directories with a suggestive title; “click on” or open the sub-directory; and then scroll through its content to view what was actually displayed there. Intentionally downloading or copying any of the pictures or videos on view would require additional steps.

**D. The Authorized Search Locations**

The cover sheet of the NIT application identifies the locations to be searched pursuant to the warrant in a sworn statement that reads as follows:

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property. . . *located in the Eastern District of Virginia*, there is now concealed (see attachment B).

Exh. B at Bates 373 (emphasis added). Consistent with this statement, the warrant itself specifies the location to be searched as “property located in the Eastern District of Virginia.” Exh. A.

The warrant then refers to “Attachment A” to more particularly describe the “property to be searched” within that district. Attachment A first lists the “TARGET WEBSITE,” “which will be located at a government facility in the Eastern District of Virginia.” *Id*. at Bates 375. As noted, “Target Website” refers to the Playpen server that had already been seized, and none of the data sought by the FBI was stored on or available from that server. “Attachment A” then lists “activating computers” as an additional place to be searched, and describes them as “those of any user or administrator who logs into the TARGET WEBSITE.” *Id*. However, the attachment does not identify any locations other than EDVA, nor does it state that “activating computers” may be located outside the district or otherwise modify the affiant’s averment on the application’s first page that searches would extend only to targets within the district.

Finally, the warrant does not incorporate the supporting affidavit by reference, and the affidavit was not physically attached to the warrant.

**E. The Search of Mr. Doe’s Home Computer**

The FBI began searching computers on February 20, the same day the NIT warrant was granted. On or about February 24, 2015, FBI agents sent the NIT malware to a computer connected to someone with the username “Jimbox” and then seized data from it.

On March 13, 2015, the FBI used some of the data it had collected from the Washington computer to prepare an administrative subpoena to Sprint for address information related to that seized data. Sprint responded with Mr. Doe’s subscriber information, name and address.

On July 28, 2015, FBI and other law enforcement agents searched Mr. Doe’s home pursuant to a second warrant issued by the Hon. XXXXXX the previous day. Pursuant to that warrant agents seized several computers, hard drives, a cellular phone and other personal property. The police also seized a XXXXXX. Mr. Doe was then detained and interrogated, during which he agreed to take a polygraph test. During this interrogation Mr. Doe, who is XX years old, reported that he has been treated for severe depression since 2011 and allegedly admitted

. Mr. Doe has never been previously charged with a sex-related offense and there is no allegation that the instant possession charges are related to any “hands-on” or production offenses.

**III. ARGUMENT**

**A**. **The NIT Warrant Was Not Supported by Probable Cause**

The NIT warrant authorized the FBI to search the computers of any and all visitors to Playpen from the moment they entered a name or password on the home page. *See* exh. B at ¶ 32 (seeking authority “to investigate any user or administrator *who logs into* the TARGET WEBSITE by entering a user name and password”) (emphasis added). The user name and password could be made up and entered on the spot, and the site did not charge any fees. Nor did it verify user information or otherwise require affirmative steps to access the site.

Because there was no particularized information in the warrant application about site visitors and it did not include an expert “collector profile,” probable cause for the computer searches turned on the contents of the home (or “log in”) page and whether it was likely that anyone who saw that page would know that its contents were illegal before proceeding to actually take a look at the contents. *United States v. Gourde*, 440 F.3d 1065, 1070 (9th Cir. 2005). While the warrant application asserted that Playpen “advertised” that it was “dedicated” to child pornography, even a cursory review of its home page shows that this is not correct. *See* exh. C.

Setting aside for the moment the inaccuracy of the warrant application, and taking it at face value, the only facts that would support the conclusion that the site was obviously dedicated to child pornography are the description of two pictures that appear on the site’s banner, “located to either side of the site name,” “depicting partially clothed prepubescent females with their legs spread apart.” Exh. B at ¶ 12.

The affiant did not claim that these pictures met the definition of illegal “lascivious” images, and in fact they do not. *See* *generally* *United States v. Battershell*, 457 F.3d 1048, 1051 (9th Cir. 2006) (photograph described as “a young female (8–10 YOA) naked in a bathtub” is “insufficient to establish probable cause that the photograph lasciviously exhibited the genitals or pubic area”); *United States v. Brunette*, 256 F.3d 14, 17 (1st Cir. 2001) (statement that images showed “‘a prepubescent boy lasciviously displaying his genitals’” was a “bare legal assertion, absent any descriptive support and without an independent review of the images, [which] was insufficient to sustain . . . probable cause”). Nor did the affiant include a copy of the home page with the warrant application so that Magistrate Judge Buchanan could assess it for herself.

As a result, the affidavit – even if it had been accurate – did not establish probable cause to search the computers of the tens of thousands of people who visited Playpen. *Compare* exh. C *with* exh. G (mainstream media pictures of child models and pageant contestants that appeared in response to a recent Google search for “child models”). And, without any pictures that are at least arguably “lascivious,” there is nothing to show that Playpen advertised or promoted itself as a child pornography site. In this regard, the rest of the facts in the affidavit about the site relates to general (and frequently erroneous) information about the Tor network; a recitation of some technical text on the home page; and the site’s contents. While the last is certainly relevant, it adds little or nothing to the probable cause analysis in this particular case because the Government chose to seek authorization to execute its searches *before* visitors entered the site and could see what it actually contained. *Compare* *Gourde*, 440 F.3d at 1070 (affidavit established that the defendant had paid for a multi-month membership after having had an opportunity to view samples of the child pornography offered on the site).

In short, given the facts alleged in the affidavit, there can be no reasonable dispute that the critical information for probable cause purposes was the claim that the site displayed “partially clothed prepubescent females with their legs spread apart” and the suggestion, at least, that these images were “lascivious” and illegal.

The law is clear, however, that when a computer search is based on someone’s mere accessing of a website, there is probable cause for a search only if the site’s illegal purpose or content is readily apparent.In *Gourde*, the Ninth Circuit carefully considered whether there was probable cause to search the computer of someone based on their membership in a site that distributed child pornography. The question of probable cause turned on how the site would appear to even a first time or casual visitor, and what Gourde had done apart from merely visiting the site that manifested his intent to view and possess child pornography. Unlike here, the site in *Gourde* was quite explicit about what it offered.

First, the name of the site was “Lolitagurls.com,” and the term “Lolita” is particularly associated with a prurient focus on young girls. *See United States v. Gourde*, 382 F.3d 1003, 1014 (9th Cir. 2004) (Gould, J. concurring in original panel decision); *see also United States v. Shields*, 458 F.3d 269, 279 (3d Cir. 2006) (warrant affidavit “explained that ‘[s]ometimes individuals whose sexual objects are minors will refer to these images as ‘Lolitas,’ a term whose etymology ‘comes from the titles of old child pornography magazines.’”).

Here, by contrast, the affiant did not allege that the site’s name had any connection to child pornography. To the contrary, the name “Playpen” is widely associated with a “men’s lifestyle” magazine that is a knock-off of Playboy (*see* exh. E); numerous strip clubs around the country, including one that advertises itself as “the premier adult entertainment strip club close to downtown Los Angeles” (*id*.); and popular, legal web sites (such as “Angel’s Playpen” and “Xtreme Playpen”) that feature far more explicit (and entirely legal) pictures of young women than appear on the site at issue here. *Compare* exhs. C *and* E.[[7]](#footnote-7)

Further, unlike Playpen’s home page, the Lolitagurls.com home page brazenly advertised the number and quality of its “Lolita pics,” including “[o]ver one thousand pictures of girls age 12-17! Naked lolita girls with weekly updates! What you will find here at Lolitagurls.com is a complete collection of young girl pics.” 440 F.3d at 1067. Hence, in stark contrast to Playpen, the site in *Gourde*, like that in *United States v. Martin*, 426 F.3d 68, 75 (2d Cir. 2005) (cited in *Gourde*, 440 F.3d at 1072 as involving “nearly identical facts”), “unabashedly announced that its essential purpose was to trade child pornography.” *See also, e.g.,* *Shields*, 458 F.3d at 278 (agreeing with *Martin*’s characterization of site as one that ““unabashedly announced that its essential purpose was to trade child pornography”); *United States v. Froman*, 355 F.3d 882, 890 (5th Cir. 2004) (similar conclusions for same “Candyman” site).

Significantly, the site in *Gourde* also charged a membership fee and visitors saw “images of nude and partially-dressed girls, some prepubescent” *before* they paid the fee and joined the site. 440 F.3d at 1067. Unlike with Playpen, which was free and immediately accessible, the court found that Gourde had demonstrated his intent to view and download child pornography because, *after* having viewed samples of the illicit pictures offered on the site, he took the additional “affirmative steps” of entering his credit card information, paying a monthly fee, and maintaining his membership for at least two months. *See id*. at 1071 (“The affidavit left little doubt that Gourde had paid to obtain unlimited access to images of child pornography knowingly and willingly, and not involuntary[il]y, unwittingly, or even passively”).

Given these facts, the court found that the warrant application in *Gourde* had demonstrated that he was not an “accidental browser” or “someone who took advantage of the free tour” offered by the site, but who, after viewing the contents, “balked at taking the active steps necessary to become a member.” *Id.* at 1070. By contrast here, the NIT warrant did nothing to distinguish between “accidental browsers” (or even people looking for legal pornography or more extreme, but still legal, fetish content) and people who, like Gourde, had indisputably viewed samples of the child pornography on offer and then chose not only to join the site, but pay for a continuing membership.

In this regard, the NIT warrant application does not allege that logging into Playpen required any significant steps, like first getting a tour of the site and then paying a membership fee. It does, however, claim that “numerous affirmative steps” were required for users to locate Playpen on the Internet, and therefore it was “extremely unlikely that any user could simply stumble upon [it] without understanding its purpose and content.” Exh. B at ¶ 10. For anyone who has even a passing familiarity with the Tor network, these statements are nonsense (and will be addressed in further detail below in connection with Mr. Doe’s request for *Franks* hearing). In fact, the discovery shows that Playpen came to the attention of law enforcement in the first place because investigators “stumbled upon it” when the site was accessible on both the regular Internet and Tor network.

Moreover, contrary to the affiant’s claim that sites cannot be found on the Tor network with the equivalent of a “Google” search (exh. B at ¶ 10), the Tor browser looks like a regular browser and there are a variety of Tor search engines.[[8]](#footnote-8) All a user need do is enter search terms for sexually oriented sites, chat rooms, or a host of other content not related to child pornography to find sites like Playpen. *See, e,g.,* <https://ahmia.fi/search> (a search engine which interfaces with both the regular Internet and allows users to use search terms to find sites on the Tor network).

The application also falsely claimed that “Tor hidden services are not indexed like web sites on the traditional Internet.” Exh. A at ¶ 10. In fact, the Tor network offers numerous “indexes,” which contain links to all sorts of sites with sexual content that may or may not be legal. *See, e.g*, <http://thehiddenwiki.org/> (the most popular Tor index, which also lists (contrary to the affiant’s claims) a variety of Tor search engines).

Finally, the court in *Gourde* relied in part on the fact that the warrant application contained a detailed collector profile that linked Gourde’s activities on the site to behavior typically associated with child pornography collectors. 440 F.3d at 1072. Here, by contrast, the warrant application made no attempt to link the act of simply visiting Playpen’s home page to specific offender characteristics. As a result, the warrant made no distinction between, on the one hand, casual or “unwitting” visitors and “accidental browsers” and, on the other, the subset of people actively seeking child pornography; instead, both groups were authorized targets of the FBI’s searches. *See United States v. Comprehensive Drug Testing*, 621 F.3d 1162, 1176 (*CDT*) (9th Cir. 2010) (“Wrongdoers and their collaborators have obvious incentives to make data difficult to find, but parties involved in lawful activities may also encrypt or compress data for entirely legitimate reasons: protection of privacy, preservation of privileged communications, warding off industrial espionage or preventing general mischief such as identity theft.”).

In short, the probable cause boundaries laid out in *Gourde*, *Martin* and elsewhere make sense, because the Internet is awash with websites that cater to every imaginable taste and fetish, much of which may be utterly repugnant, but is nonetheless legal and even constitutionally protected. *See Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 245 (2002) (it is “well established that speech may not be prohibited because it concerns subjects offending our sensibilities”); *McIntyre v. Ohio Elections Commission*, 514 U.S. 334, 355 (1995) (the right to anonymity while engaging in speech related activities – such as using Tor and Playpen’s chat and messaging services – “is an aspect of free speech protected by the First Amendment”).

As the Second Circuit recently concluded when reversing the conviction of a police officer charged with planning to attack and cannibalize women, “Although it is increasingly challenging to identify that line [between fantasy and intent] in the Internet age, it still exists and it must be rationally discernible in order to ensure that ‘a person’s inclinations and fantasies are his own and beyond the reach of the government.’” *United States v. Valle*, 807 F.3d 508, 511 (2d Cir. 2015) (reversing conviction of defendant known as “Girlmeat Hunter” who engaged in gruesome exchanges on fetish websites) (citation omitted). The court went on to emphasize that “[w]e are loath to give the government the power to punish us for our thoughts and not our actions. That includes the power to criminalize an individual’s expression of sexual fantasies, no matter how perverse or disturbing.” *Id*. (citation omitted).

With these principles in mind, the NIT warrant application was a very slim reed on which to hang a sweeping authorization (as the Government interprets the warrant) to search 100,000 or more computers. This is especially true given that the application cannot be taken at face value. When the Court considers what the site actually looked like, and the lack of information showing that the site advertised itself as a source of child pornography, there can be no reasonable dispute that the issuing magistrate would not have granted the warrant if she had been presented with the complete and accurate facts that were known to the FBI at the time.

**B**. **The Court Should Hold a *Franks* Hearing Because the NIT Affidavit Contains, at a Minimum, Recklessly Misleading Statements and Omissions.**

The facts alleged in the warrant application cannot be taken at face value, however, because several critical allegations were false or misleading. In *Franks v. Delaware*, 438 U.S. 154, 156 (1978), the Supreme Court held that “where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant’s request.”

The doctrine applies to omissions, not just false statements. *United States v. Stanert*, 762 F.2d 775, 780-81 (9th Cir.), *amended by* 769 F.2d 1410 (1995). It also includes “recklessly fail[ing] to verify” information that is material to a finding of probable cause. *United States v. Meling*, 47 F.3d 1546, 1553 (9th Cir. 1995). And the doctrine further applies when the affiant “intentionally or recklessly omitted facts required to prevent technically true statements in the affidavit from being misleading.” *Id.* at 781. The proper approach is “to delete false or misleading statements and insert the omitted truths revealed at the suppression hearing.” *United States v. Ippolito*, 774 F.2d 1482, 1486 n. 1 (9th Cir. 1985) (which another circuit refers to as “reconstructive surgery”; *see Wilson v. Russo*, 212 F.3d 781, 789 (3d Cir. 2000)).

In this case, the false and omitted statements were plainly material. In fact, the description of the home page was a pivotal component of the affiant’s allegations in support of probable cause. The affiant’s burden, after all, was not just to show that Playpen contained child pornography. If that is all that were required, then someone could have his home searched simply for entering a bookstore that sold child pornography from under the counter, even though all he was looking for was a copy of Playboy.

Instead, in order to support a sweeping authorization to search the computers of anyone who accessed the site, the Government aimed to persuade the Magistrate Judge that the site was not only “dedicated” to child pornography, but that this purpose would be apparent to anyone who viewed its public home page and therefore would know what he or she was getting into. The affidavit accomplished that (if it did so at all) by including a patently inaccurate description of the site in the supporting affidavit, despite the fact that the FBI well knew before applying for the warrant that it was inaccurate. These facts alone warrant a *Franks* hearing. *See also* *CDT*, 621 F.3d at 1178 (“A lack of candor in [any] aspect of the warrant application must bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized data”) (Kozinski, J., concurring).

To make matters worse, the false description of the home page was accompanied by other lesser but nonetheless false statements and omissions that, taken as a whole, resulted in a highly confusing and misleading affidavit.

To begin, the affiant claimed that “the entirety” of Playpen is “dedicated to child pornography.” Exh. B at ¶ 27. As noted above, the content of the site is not a critical part of the probable cause analysis because the NIT searches were predicated on facts ostensibly showing that visitors would know its illegal purpose before logging in, given the point in time that the searches could be executed. Nevertheless, this characterization of the site’s content is plainly false, as revealed by its table of contents and the discovery.

In addition, the affiant was either woefully uninformed or recklessly misleading about how sites are found on the Tor network, going so far as to claim that there is no such thing as a Tor equivalent of a Google search engine. These statements, which make it appear that anyone who found Playpen must be determinedly seeking out child pornography, are simply not true. To the contrary, once someone has downloaded the free Tor browser package that connects them to the network they can explore it with a Tor search engine similar to Google or Bing. *See, e.g*, <https://ahmia.fi/search>. Using search terms for legal content, such as “sex chat” or “teen erotica,” can readily lead Tor browsers to a variety of sites like Playpen. *See* *generally* *United States v. Hill*, 459 F.3d 966, 970 (9th Cir. 2006) (“Child pornography is a particularly repulsive crime, but not all images of nude children are pornographic.... Moreover, the law recognizes that some images of nudity may merit First Amendment protection because they serve artistic or other purposes, and possessing those images cannot be criminal”).

Further, while describing the site as “dedicated” in its “entirety” to child pornography, the affiant fails to mention that one of the most prominent aspects of site is its chat forum. *See* exh C. This omission implicates substantial First Amendment rights that the Magistrate Judge should have been allowed to consider when determining how much authority to allow the FBI in targeting visitors to the site. *See In re Anonymous Online Speakers,* 661 F.3d 1168, 1173 (9th Cir. 2011) (“Although the Internet is the latest platform for anonymous speech, online speech stands on the same footing as other speech—there is ‘no basis for qualifying the level of First Amendment scrutiny that should be applied’ to online speech”) (quoting *Reno v. Am. Civil Liberties Union,* 521 U.S. 844, 870 (1997)).

These facts, coupled with the absence of any images of “prepubescent” girls or even clear indication that the site contains pornographic pictures (let alone child pornography), are inconsistent with the portrait the affiant was trying to paint of a site that “advertises” itself as “dedicated” to child pornography.

The Government also devoted a substantial portion of the application to describing commonplace features of the site, while at least suggesting that these features were indicative of criminality. For example, the affiant stated that the site “allows users of the TARGET WEBSITE to upload links to images of child pornography that are accessible to all registered users of the TARGET WEBSITE.” Exh. A ¶ 23. This statement is both true and calculated to mislead. The same link and image upload capabilities described by the affiant are basic features of myriad web sites that enable users to post messages and pictures, including everything from pictures of baked goods (*see, e.g*, epicurious.com) to YouTube videos.

Likewise, the affidavit misleadingly states that the ability of users to exchange names and messages on the site are features “commonly used by subjects engaged in the online sexual exploitation of children.” Exh. A ¶ 15. These very same features are offered by Twitter and Facebook, among many others. Suggesting that they are in any way indicative of criminality is similar to asserting that bank robbers “commonly” use cars to make a getaway. Millions of innocent people have cars, and the mere fact that someone has a car does not remotely support the conclusion that he or she is likely to be a bank robber.

In sum, the application’s false description of Playpen’s home page, compounded by highly inaccurate statements about how the Tor network functions and a cloud of misleading technical jargon, should persuade the Court that a *Franks* hearing is amply warranted in this case.

**C. The NIT Warrant Was Overbroad**

The NIT warrant application’s probable cause shortcomings are compounded by the extraordinary scale of the search authorization that the Government is claiming. As the Ninth Circuit has explained when it comes to the question of whether a warrant is overbroad, there is a direct relationship between the scope of the search authorized by a warrant and the extent to which probable cause for the search has been established; the broader the search, the more extensive the showing of probable cause must be. *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006) (“Search warrants must be specific. ‘Specificity has two aspects: particularity and breadth. Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based.’”) (citations omitted).

In this case, the Government will be advocating for approval of an unprecedentedly sweeping exercise of search and seizure powers. Unlike a typical search warrant based upon facts establishing probable cause to search a particular location, the warrant purportedly gave the FBI broad discretion in deciding when and against whom to deploy the NIT. Specifically, the warrant authorized NIT searches any time someone accessed Playpen’s home page, regardless of whether they merely utilized its “chat” forum or their actual activities on the site. *See generally* Kevin Poulsen, *Visit the Wrong Website, and The FBI Could End Up in Your Computer*, Wired.com, August 5, 2014 (although targeted use of “malware” by the FBI is not new, “[w]hat’s changed is the way the FBI uses its malware capability, deploying it as a driftnet instead of a fishing line”).[[9]](#footnote-9)

As a result, the NIT warrant may fairly be characterized as the Internet age equivalent of a general warrant, allowing the FBI to search tens of thousands of computers for which probable cause to search was not established. Worse yet, the warrant could easily have been narrowed to authorize searches of only those site visitors who viewed or downloaded illegal pornography, an appropriately circumscribed line to draw given that illicit content was contained in specific sub-directories on the site. Since the FBI could send its malware to anyone who logged into the site, the warrant could simply have required the FBI to target only those people who “clicked” on particular sub-directories with illegal content or particular pictures or links in those sub-directories. Indeed, in a footnote, the affiant acknowledges that the FBI could do exactly that, yet the warrant does nothing to particularize or narrow the set of visitors who would be subjected to searches. Exh. B at ¶ 32, n. 8.

It is this type of narrowing of computer searches, or search protocols, that the Ninth Circuit has admonished judges to impose when issuing warrants to seize electronic data. *See CDT*, 621 F.3d 1162 (disapproving of “deliberate overreaching” by the Government in seizing electronic data, *id*. at 1172 , and requiring judges to exercise “greater vigilance” when approving computer search warrant applications, *id*. at 1177). Such specificity requirements “prevent[] officers from engaging in general, exploratory searches by limiting their discretion and providing specific guidance as to what can and cannot be searched and seized.” *United States v. Adjani*, 452 F.3d 1140, 1147-48 (9th Cir. 2006). Hence, “[a] warrant must not only give clear instructions to a search team, it must also give legal, that is, not overbroad, instructions.” *United States v. SDI Future Health, Inc.,* 568 F.3d 684, 702-03 (9th Cir. 2009), quoting *In re Grand Jury Subpoenas,* 926 F.2d 847, 857 (9th Cir. 1991); *see also, generally, Ashcroft v. al-Kidd,* 131 S. Ct. 2074, 2084 (2011) (“The Fourth Amendment was a response to the English Crown’s use of general warrants, which often allowed royal officials to search and seize whatever and whomever they pleased while investigating crimes”). Nevertheless, in this case, the FBI sought the broadest possible search authorization, encompassing many thousands of targets, and the warrant itself did nothing to narrow or focus that authorization.

In short, the NIT warrant implicates the Fourth Amendment’s core purpose of guarding against overbroad and unreasonable searches for several reasons. According to the Government, it authorized the FBI to execute searches on a population of potential targets so large that it exceeds the population of Olympia, Washington, and many other small cities. If the Government is correct, the warrant granted this unprecedented search and seizure authority based on a showing of probable cause that, even taking the facts in the warrant application at face value, was insufficient. With the *Franks* violations taken into consideration, the overbreadth of the warrant is even more striking and, standing alone, warrants suppression. *United States v. Kow*, 58 F.3d 423 (9th Cir. 1995) (rejecting good faith exception and affirming suppression order for search undertaken pursuant to an overbroad warrant).

**D. The NIT Warrant was an Anticipatory Warrant and, Regardless of the False and Misleading Statements in the Supporting Affidavit, the “Triggering Event” for the Computer Searches Failed.**

The Government has described the NIT warrant as an anticipatory warrant. This is because the warrant prospectively authorized searches whenever unidentified Playpen visitors signed on to the site, with the “triggering event” for those searches being the act of accessing the site. *See* exh. B at ¶ 32 (requesting authority “to use the NIT. . . to investigate any user or administrator *who logs into* the TARGET WEBSITE by entering a user name and password”) (emphasis added). As the Ninth Circuit has explained, “[t]he execution of an anticipatory search warrant is conditioned upon the occurrence of a triggering event. *If the triggering event does not occur, probable cause to search is lacking.*” *United*  *States v. Vesikuru*, 314 F.3d 1116, 1119 (9th Cir. 2002) (emphasis added).

In this case, there was probable cause to search the computers of everyone who signed into Playpen (the triggering event) only if the site continued to “unabashedly announce” that it was dedicated to child pornography. Assuming, for the sake of argument, that the warrant application’s description of pornographic pictures on the home page had established probable cause to believe that anyone who entered the site was a legitimate search target, the foundation for that conclusion was undermined when that description proved to be inaccurate.

Without illegal images on the public home page, all that remains to establish probable cause is the technical verbiage on the home page, which is not indicative of illegal activity; general and erroneous assertions about how sites can be found on the Tor network; and the allegations about the site’s content. The content, moreover, is largely irrelevant because the warrant authorized searches before users could even see that content.

Given these facts (or lack of them), there can be no reasonable dispute that the home page as it actually appeared when the warrant was approved and the searches were executed contains little, if anything, that would lead an unwitting visitor to believe that Playpen was more than a common pornography site or sexually oriented chat room. As a result, the triggering event as established in the warrant application could not, and did not, occur. And, since the triggering event could not occur, any searches based on the NIT warrant inevitably exceeded the scope of its authorization.

Nevertheless, without alerting the Virginia court to its errors or submitting a revised warrant application, the Government proceeded to search the computers of site visitors for at least two more weeks as if nothing had changed. Regardless of whether this sequence of events was the result of intentional or reckless conduct, or is attributable to mere carelessness, key facts that the Government had relied on to establish probable cause and the triggering event for the searches no longer existed by the time those searches were executed. Consequently, when the Government proceeded with the NIT searches anyway, it was acting outside the scope of the warrant, and suppression is required. *See Vesikuru*, 314 F.3d at 1123 (if the “triggering events did not occur, the warrant was void, and evidence gathered from the search would have to be suppressed.”).

**E. The NIT Search of Mr. Doe’s Washington Computer was Not Authorized by the Warrant.**

Based on the express language of the NIT warrant itself, the Court can and should grant an order of suppression for the simple reason that the FBI searched the wrong location.

To begin, the cover sheet of the NIT application (the first thing the issuing judge would have looked at to determine the location of the proposed search) reads as follows:

I, a federal law enforcement officer or an attorney for the Government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property. . . *located in the Eastern District of Virginia*, there is now concealed (see attachment B).

Consistent with this sworn statement, the NIT warrant itself authorizes searches of “person or property located in the Eastern District of Virginia.” Exh. A at Bates 135.

To state the obvious, when a warrant authorizes searches in one location, it does not authorize searches in other locations. *Walter v. United States*, 447 U.S. 649, 656 (1980) (“When an official search is properly authorized – whether by consent or by the issuance of a valid warrant – the scope of the search is limited by the terms of its authorization.”); *see also, e.g., Simmons v. City of Paris, Tex.*, 378 F.3d 476 (5th Cir. 2004) (warrant for 400 N.W. 14th Street did not justify search of 410 N.W. 14th Street; affirming denial of qualified immunity for officers involved in search); *Pray v. City of Sandusky*, 49 F.3d 1154 (6th Cir. 1995) (warrant for 716 ½ Erie Street, upper level of a duplex home, did not justify search of 716 Erie Street, lower level of the duplex; affirming denial of qualified immunity for officers involved in search).

Here, the FBI violated the express terms of the NIT warrant by searching a location in Washington State (Mr. Doe’s home computer). In response, the Government will no doubt note that the warrant’s “Attachment A” (“Place to be Searched”) refers to the “activating computers” of “any user or administrator who logs into” Playpen. However, this attachment is incorporated by the warrant solely to identify “the property to be seized” that is “now concealed” in the Eastern District of Virginia, and does not alter the specific location stated on the face of the warrant itself. Consistent with this conclusion, the attachment itself does not reference any locations other than the EDVA or otherwise expand the geographic boundary imposed by Magistrate Judge Buchanan on the face of the warrant.

Accordingly, while a fair reading of the warrant and attachment does authorize searches of “activating computers” wherever they may be located in the Eastern District of Virginia, there is nothing within the four corners of the warrant that alters its plain language or can reasonably be construed to expand the search authorization to anywhere in the world. Suppression is required for all data that was seized outside of the warrant’s express and limited authorization. *United States v. Sedaghaty*, 728 F.3d 885, 913 (9th Cir. 2013) (although affidavit arguably described broader category of items to be seized, “the language of the warrant controls” and suppression is required for any evidence that exceeds the scope of the authorization in the warrant itself).

**F. If the Warrant Could be Construed to Allow Searches Anywhere, Then the Warrant Would Violate Rule 41 and Suppression Would Still be Required.**

If the Government nevertheless maintains that the NIT warrant authorized searches of computers across the United States and around the world, despite the plain language of the warrant itself, then it must confront a different set of issues that also lead to suppression.

Pursuant to Fed. R. Crim. P. 41, searches in one district cannot be executed with a warrant that has been issued in another district, with very limited exceptions that do not apply in this case. *See generally* *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013) (“*In re Warrant”*) (rejecting a NIT malware warrant application because issuing the warrant would have violated Rule 41). These jurisdictional limitations are not mere technical requirements or just procedural. Rather, Rule 41 has the force of law, and this law is rooted in the Fourth Amendment’s prohibition on general warrants and its restraints on governmental overreaching when exercising its law enforcement powers. *See* 18 U.S.C. § 3103; *In re. Warrant*, 958 F. Supp. 2d at 758.

With these principles in mind, the Ninth Circuit requires suppression of evidence obtained through searches that violate Rule 41 if any one of the following three things occurred: (1) the defendant was “prejudiced, in the sense that the search would not have occurred or would not have been so abrasive if law enforcement had followed the Rule;” (2) the violation of the rule is one of “constitutional magnitude;” *or* (3) officers acted in “intentional and deliberate disregard” of a provision in the Rule. *United States v. Weiland*, 420 F.3d 1062, 1071 (9th Cir. 2005) (citations omitted); *see also* *United States v. Martinez-Garcia,* 397 F.2d 1205, 1213 (9th Cir. 2005) (same); *United States v. Glover*, 736 F.3d 509, 515 (D.C. Cir. 2014) (the language of Rule 41(b)(2) is “crystal clear” and a “jurisdictional flaw” in the warrant cannot be excused as a “technical defect”)*.*

The careful analysis in *In re Warrant* provides a helpful framework for considering the potential Rule 41 issues. There, the Government was investigating a fraud and identity theft case perpetrated with an “unknown computer at an unknown location.” 958 F. Supp. 2d at 755. Like the warrant here, the warrant sought in that case would have “surreptitiously install[ed] data extraction software” on a computer somewhere in the world using an older version of the NIT that was used to seize evidence from Mr. Doe’s home computer. *Id*. The *In re Warrant* was both broader and narrower than the one in Mr. Doe’s case. It was broader in that it sought authorization “not only to extract certain stored electronic records but also to generate user photographs and location information[.]” *Id.* at 755. However, the breadth of the search was not part of the court’s analysis. The request was also narrower than that here, because it was aimed at one computer, rather than as many as 100,000 computers.

In *In re Warrant*, the Government primarily relied on Rule 41(b)(1), which “allows a ‘magistrate judge with authority in the district ... to issue a warrant to search for and seize a person or property located within the district.’” *In re Warrant,* 958 F. Supp. 2d at 756 (quoting Rule 41). The Government’s argument was puzzling because it had conceded that the location of the target computer was unknown (as it has likewise conceded that the locations of the computers targeted in this case were unknown). Nevertheless, the Government posited that “this subsection authorizes the warrant ‘because information obtained from the Target Computer will first be examined in this judicial district.’” *Id*. (quoting warrant application).

Not surprisingly, the court rejected the Government’s novel theory that a search did not occur until investigators “examined” whatever information they had already seized. “Contrary to the current metaphor often used by Internet-based service providers, digital information is not actually stored in clouds; it resides on a computer or some other form of electronic media that has a physical location.” *Id*. at 757. The search and seizure of data occurs “not in the airy nothing of cyberspace, but in physical space with a local habitation and a name.” *Id.* Accordingly, the warrant sought by the Government would have permitted “FBI agents to roam the world in search of a container of contraband, so long as the container is not opened until the agents haul it off to the issuing district.” *Id.* at 757. Since the search for and collection of digital evidence would occur on a computer that may be located outside the district, the court had little difficulty concluding that a warrant was not permitted under Rule 41(b)(1) (or any other provision of the Rule), regardless of where seized data was later reviewed.

In this case, the Government’s warrant application was much less forthright about its actual targets, and it will no doubt seek to use its own lack of clarity to persuade this Court that it can retrofit the warrant to accommodate the search of Mr. Doe’s computer. But there is no escaping the fact that the NIT warrant affidavit plainly states that the Government wanted authorization to search a “person or property in the Eastern District of Virginia.” It is only upon a close reading of the entire application that it becomes clear that the FBI server in Virginia that was running the “Target Website” (*i.e*. Playpen) was not a search location at all, and the actual “place to be searched” could potentially include thousands of “activating computers” scattered around the world. Given these facts, the conclusion in *In re Warrant* that “the Government’s application cannot satisfy the territorial limits of Rule 41(b)(1)” is equally applicable here. *Id.* at 757.

Of course, *In re Warrant* is not controlling precedent. But its analysis is not just persuasive, it follows directly from the plain wording of Rule 41 and from the nature of what the Government now says it asked Magistrate Judge Buchanan to authorize. The conclusion is as manifest here as it was in *In re Warrant*: “the Government’s application cannot satisfy the territorial limits” of Rule 41. *Id.* at757.

Given the facts and law, it is clear that Magistrate Judge Buchanan was presented with what appeared to be a request to search “activating computers” in her district (consistent with the affiant’s statement identifying the search locations, exh. B at Bates 373) and that, consistent with Rule 41, she approved such searches. It goes virtually without saying that this plain reading of both the affiant’s statement on the first page of the application and the warrant itself does not include authorization to search a computer in Seattle, Washington.

Nevertheless, the Government is likely to argue that the warrant application actually sought authorization to search computers anywhere in the world by citing a statement (on page 29 of the 31 page affidavit) that “the NIT may cause an activating computer – wherever located – to send” seized data to an FBI computer. Exh. B at ¶ 46(a). But this argument is unavailing. Even assuming that such a passing reference was sufficient to forthrightly apprise the Magistrate Judge that the FBI intended to search computers anywhere in the world, it does not change the fact that she decided to issue a more circumscribed warrant. *See* *Sedaghaty*, 728 F.3d at 913 (even where the affidavit was expressly incorporated into the warrant - which it was not in this case - the court stated: “May a broad ranging probable cause affidavit serve to expand the express limitations imposed by a magistrate in issuing the warrant itself? We believe the answer is no. The affidavit as a whole cannot trump a limited warrant.”).

Regardless of what is in the application, the only way to construe the warrant so that it is consistent with Rule 41 is to presume that Magistrate Judge Buchannan followed the rule, and did exactly what she was supposed to do consistent with the principles summarized in *CDT*; she gave authorization only to targets within her district, which still allowed the FBI to pursue numerous investigations and continue to build its case to the point where it could apply for additional NIT warrants in other districts. *See* *CDT*, 621 F3d at 1177 (Requiring “greater vigilance on the part of judicial officers in striking the right balance between the government’s interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures. The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect”); s*ee also* *Kentucky v. King*, 563 U.S. 452 (2011) (“a warrant may not be issued unless probable cause is properly established *and* the scope of the authorized search is set out with particularity”) (emphasis added).

In short, even if the FBI had been perfectly clear about its intention of exercising unprecedently sweeping search and seizure powers, *and* the warrant application could be considered when construing the warrant itself, the Government would still be asking this Court to second-guess the Magistrate Judge’s decision to issue a more limited warrant and retroactively approve the search of Mr. Doe’s computer. The defense urges the Court to reject that invitation.

**1. A Violation of Rule 41 in This Case Requires Suppression**

The court in *In re Warrant* refused to issue a warrant that violated Rule 41 and therefore did not address the question of what remedy is required when a warrant has been issued (as the Government would have it) that violates the Rule. In this case, the law is clear that suppression would be the required remedy. As cited above:

Suppression of evidence obtained through a search that violates Federal Rule of Criminal Procedure 41 is required only if: 1) the violation rises to a ‘constitutional magnitude;’ 2) the defendant was prejudiced, in the sense that the search would not have occurred or would not have been so abrasive if law enforcement had followed the Rule; or 3) officers acted in ‘intentional and deliberate disregard’ of a provision in the Rule.

*Weiland*, 420 F.3d at 1071 (citation omitted). Moreover, the “good faith” exception to the exclusionary rule does not apply if the rule violation lies in the execution of the warrant or is otherwise “the fault of the officers.” *United States v. Gantt*, 194 F.3d 986, 1006 (9th Cir. 1999), *overruled on other grounds, United States v. W.R. Grace,* 526 F.3d 499 (2008). Although running afoul of any one of the *Weiland* prongs requires suppression, the Government in this case has achieved a trifecta.

First, Mr. Doe was indisputably prejudiced “in the sense that the search would not have occurred or would not have been so abrasive if law enforcement had followed the Rule[.]” Had the Government complied with the NIT warrant, it would have searched only “activating computers” in the Eastern District of Virginia. Consequently, “the search would not have occurred” in this case and Mr. Doe would not have been prejudiced.

Conversely, if Magistrate Judge Buchanan had in fact issued a warrant that authorized searches anywhere (as the Government will no doubt try to argue), then that warrant would have violated Rule 41 and Mr. Doe would have been prejudiced because the search could not have occurred without that violation.

As a result, no matter how the Government tries to slice the NIT warrant and supporting affidavit, it arrives at the same dilemma: either the search violated the particularized geographic limits set forth in the warrant itself, or the warrant can somehow be expansively construed to allow for myriad searches anywhere, in which case it violates Rule 41. Either way, suppression is required. *See also* *United States v. Krueger*, 998 F. Supp. 2d 1032 (D. Kan. 2014) (where Government obtained warrant in Kansas for a house in Oklahoma, the “court finds that defendant has shown prejudice in that if Rule 41(b)(2) ‘had been followed to the letter’” the warrant would not have been issued and that this prejudice required suppression) (citation omitted).

In *Michaud*, the court concluded that “the NIT warrant did technically violate” Rule 41, but it did not address *Gantt* and declined to follow *Weiland* and *Martinez-Gonzalez* by granting suppression. Michaud Order at 13. The court attributed to the defense the view that “defendants suffer prejudice whenever a search occurs that violates Rule 41(b),” which “makes no sense” because then “all searches executed on the basis of warrants in violation of Rule 41(b) would result in prejudice, no matter how small or technical the error might be. Such an interpretation would defeat the need to analyze prejudice separately from the Rule 41(b) violation.” Michaud Order at 14.

That is an incorrect understanding and application of both the defense’s argument and the controlling Ninth Circuit authority, neither of which lead to the result the court posited.

The question of prejudice, as stated in *Weiland*, is whether the search at issue would still have occurred if the Rule had been complied with. Contrary to the *Michaud* Order, and consistent with the Ninth Circuit’s view of prejudice, the issue is whether the rule violation was incidental to the search, or whether instead the search would not have happened at all “but for” the violation. *See*, *e.g,.* *United States v. Williamson*, 439 F.3d 1125 (9th Cir. 2006) (agents did not provide copy of warrant to the person at the premises, but they did not act in deliberate disregard of the Rule and non-compliance with the rule did not affect the validity of the search itself).

In this case, by contrast, compliance with Rule 41 would have meant searching only locations within the district of the authorizing magistrate, thereby excluding Mr. Doe’s home computer entirely. Thus, “the search would not have occurred. . . if the rule had been followed,” *Weiland*, 420 F.3d at 1071, and suppression is plainly required under the controlling Ninth Circuit authority.

In addition to establishing prejudice as defined in *Weiland*, Mr. Doe is also entitled to relief on the independent ground that a violation of Rule 41 in this case would be of “constitutional magnitude.” 420 F.3d at 1071. “Constitutional magnitude” in the Rule 41 context is not clearly defined in *Weiland* or elsewhere. However, it appears to include jurisdictional flaws and other fundamental, non-ministerial violations. *See Glover*, 736 F.3d 509 at 515 (the language of Rule 41(b)(2) is “crystal clear” and a “jurisdictional flaw” in the warrant cannot be excused as a “technical defect”)*.*

Moreover, courts have long recognized that protection of the home, where Mr. Doe had his computer, and maintaining the privacy of the personal “papers and effects” now commonly stored on computers, lies at the heart of the guarantees afforded by the Fourth Amendment. *See*, *e.g.*, *Payton v. New York*, 445 U.S. 573, 589–90 (1980); *accord*, *United States v. Becker*, 23 F.3d 1537, 1539 (9th Cir. 1994) (“[t]he sanctity of a person’s home, perhaps our last real retreat in this technological age, lies at the very core of the rights which animate the [fourth] amendment”) (citation omitted).[[10]](#footnote-10) Endorsing governmental efforts to ignore or circumvent the limits imposed by the Rule and execute a potentially unlimited number of searches anywhere in the world also implicate the Fourth Amendment’s basic particularly requirements. *See In re Warrant*, 958 F. Supp. 2d at 758 (“This particularity requirement arose out of the Founders’ experience with abusive general warrants”). Under these circumstances, Mr. Doe submits that suppression is appropriate on the independent ground that the rule violation was of “constitutional magnitude.”

Finally, there is substantial evidence that the Government acted with deliberate disregard of Rule 41 in seeking a warrant that it now claims allows for searches anywhere. *See Gantt*, 194 F.3d at 1005 (because agents’ refusal to provide copy of warrant to its subject was deliberate, court did not need to “consider whether the violation was ‘technical’ or ‘fundamental’”; “Our Rule 41(d) jurisprudence requires suppression under these circumstances”). There is no credible way to interpret the Rule that would allow dragnet searches of computers outside the authorizing district. This conclusion is self-evident from the plain language of the Rule, even without reference to the analysis in *In re Warrant*, but in fact the Government was acutely aware of that decision and its implications at the time it submitted the NIT warrant application.

Specifically, several months after *In re Warrant* was decided, the Department of Justice (DOJ) began seeking amendments to Rule 41 that would allow courts to issue warrants for data searches outside an issuing court’s district. DOJ cited the rejection of its warrant application in *In re Warrant* as a reason for changing the rule. *See* September 18, 2013 letter from Acting Asst. Attorney General Mythili Raman to the Hon. Reena Raggi, Chair, Advisory Committee on the Criminal Rules (available at: [www.uscourts.gov/file/15534/download](http://www.uscourts.gov/file/15534/download), at p. 172) (minutes and records of the Advisory Committee’s April 7-8, 2014 meeting). In its proposal to amend Rule 41, DOJ expressed its view that the Rule and its application in case like *In re Warrant* was “an unnecessary obstruction” to the kind of search that occurred here, one that needed to be “remove[d].” *Id*. at 173. Given these statements, there can be no credible dispute that DOJ knew that it was running afoul of Rule 41 in seeking a warrant that had no particularized locations or jurisdictional limitations at all. *See also United States v. Slaey*, 433 F. Supp. 2d 494, 499 (E.D. Pa. 2006) (suppressing evidence when prosecutor obtained magistrate’s authorization not to leave attachments to the warrant with the subject because “it was not reasonable for the agent to rely on a Magistrate Judge’s order authorizing him to disregard Rule 41(f)(3)(B)”).

The proposed rule amendments are still under review, and Congress and the Supreme Court will ultimately determine whether they should be adopted. Meanwhile, of course, the law remains unchanged, and the Government is not free to ignore the law simply because it disagrees with it. Nor should this Court countenance any attempt by the Government to obtain the Court’s endorsement of actions undertaken by DOJ and the FBI in defiance of the law as it now stands.

**IV. CONCLUSION**

The search of Mr. Doe’s home computer was undertaken as part of an unprecedentedly sweeping and dragnet search and seizure operation that targeted 100,000 or more private computers throughout the United States and elsewhere. The warrant application that the Government has relied on for these searches did not establish probable cause, and in fact the FBI made false statements and withheld information from the issuing judge that was material to determining probable cause.

Moreover, even if there had been probable cause, the Magistrate Judge who issued the warrant expressly limited the geographic scope of her search authorization to the Eastern District of Virginia. The Government, however, elected to blithely ignore both this limited authorization and the requirements of Fed. R. Crim. P. 41, and search computers wherever it chose to do so. Accordingly, the Court should suppress all evidence seized during the February, 2015, search of Mr. Doe’s home computer and all fruits of that search.

Dated this 22nd day of February, 2015.

Respectfully submitted,

*s/ Colin Fieman*

*s/ Mohammad Hamoudi,*

Attorneys for JOHN DOE

**CERTIFICATE OF SERVICE**

I hereby certify that on February 22, 2016, I electronically filed the foregoing Motion and Memorandum in Support of Motion to Suppress Evidence, Affidavit of Colin Fieman and Proposed Order with the Clerk of the Court using the CM/ECF system which will send notification of such filing to all parties registered with the CM/ECF system.

s/ *Amy Strickling*

Amy Strickling, Paralegal

Federal Public Defender Office

1331 Broadway, Suite 400

Tacoma, WA 98402

253-593-6710 voice

253-593-6714 facsimile

1. As of the filing of this motion, there are at least five Playpen cases pending in the Western District of Washington. On January 28, 2016, the Hon. Robert J. Bryan issued an order denying motions to suppress evidence in the first of these cases, *United States v. Michaud*, CR15-05351RJB. The findings and conclusions in that order, which the court has described as a “narrow ruling,” will be briefly discussed and distinguished in this motion. [↑](#footnote-ref-1)
2. Available at: <http://www.theguardian.com/technology/2014/jun/05/guardian-launches-securedrop-whistleblowers-documents> [↑](#footnote-ref-2)
3. Available at: <http://www.nytimes.com/2010/12/19/magazine/19FOB-Medium-t.html?_r=0> [↑](#footnote-ref-3)
4. A “server” is basically a computer that stores data for other computers, connects individual computers to Internet networks, and runs various programs that allows web sites to connect to the Internet. *See* exh. B at ¶ 5(e); <http://techterms.com/definition/server>. [↑](#footnote-ref-4)
5. The FBI also obtained a separate authorization pursuant to 18 U.S.C. § 2518 (commonly referred to as “Title III” or “the Wiretap Act”) to intercept electronic communications on Playpen’s private chat and messaging services between unknown “target subjects” or “unidentified administrators and users.” This authorization was apparently sought because 18 U.S.C. § 2511 generally prohibits electronic communication service providers from monitoring communication that take place on their services, and the FBI became the service provider for Playpen’s communication services after February 19, 2015. [↑](#footnote-ref-5)
6. In the *Michaud* order, the Court erroneously stated that an FBI Special Agent involved in the Florida search “saw the newer version of [Playpen’s] main page but did not notice the picture changes.” *Michaud* Order at 6. In fact, the agent had testified that he was aware of the change, but “it did not jump out to me as a significant change to the web site” and it was not his “intent that the change to the logo be omitted from the NIT warrant.”*Michaud*, January 22, 2016 Hearing Transcript at 87-92. Regardless of the Agent’s subjective intentions, it is undisputed that the FBI was aware prior to its application for the NIT warrant that the description of the site in that application was inaccurate. [↑](#footnote-ref-6)
7. In the *Michaud* order, the court concluded that the name “Play Pen” was “suggestive” of child pornography. *Michaud* Order at 24. The basis for this conclusion is unclear, since the NIT affidavit does not claim that the name is suggestive and the evidence shows that “Playpen” is commonly used in connection with legal “adult” entertainment. [↑](#footnote-ref-7)
8. See https://www.torproject.org/projects/torbrowser.html.en [↑](#footnote-ref-8)
9. Available at: http://www.wired.com/2014/08/operation\_torpedo/ [↑](#footnote-ref-9)
10. In this regard, the *Michaud* court’s conclusion that people do not have a privacy interest in data seized from inside their homes because that data could “eventually…have been discovered” from third parties does not make sense. *See* Michaud Order at 14. In fact, the NIT warrant application explains that the data could *not* be obtained from either third parties or Playpen’s server, which was the whole reason for doing the NIT searches. *See* exh. B at ¶¶ 8-9, 29. More basically, the privacy interest at stake is not just the data itself, but the fact that the Government transgressed the boundaries of Mr. Doe’s homes in order to obtain it. *See, e.g*., *Kyllo v. United States,* 533 U.S. 27, 37 (2001) (The “Fourth Amendment’s protection of the home has never been tied to measurement of the quality or quantity of information obtained” during a residential search). [↑](#footnote-ref-10)