UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

vs. Case No. 16-CR-38 (DEJ)

MARCUS A. OWENS,

Defendant.

MOTION TO SUPPRESS

Marcus Owens, by counsel, respectfully moves the Court under Rule 12(b)(3)(C) for an order suppressing all evidence seized from his home computer by the FBI on or about February 25, 2015, as well as all fruits of this search, including the results of later searches and his statements.

Introduction

On February 25, 2015, government agents seized evidence from Mr. Owens's home computer including an "internet protocol" (IP) address and other electronic data using a "Network Investigative Technique" (NIT). *See* Ex. A, EDWI Search Warrant and Supporting Application, at ¶27. This NIT is a type of computer program commonly referred to as "malware" that was secretly sent by FBI agents in Virginia to Mr. Owens's computer in Kenosha, Wisconsin.

Federal Defender Services
of Wisconsin, Inc.

The NIT changed and overrode security settings on Mr. Owens's computer, allowing the FBI to remotely search for and collect data from the computer's hard drive. Then the NIT transmitted that data to FBI agents in Virginia. Roughly a year later, the FBI used this information to obtain a second search warrant to search Mr. Owens' home and any digital storage devices found there. *See* Ex. A. Mr. Owens made uncounseled statements to law enforcement at that time, was subsequently arrested, and then again made uncounseled statements.

This motion presents five specific grounds for suppression.

First, the FBI remotely searched Mr. Owens' home computer pursuant to a warrant that failed to establish probable cause. As set forth below, the government sought authorization to search the computers of anyone who entered a website called "Playpen." See Ex. B, NIT Warrant and Supporting Application. Probable cause for these searches turned on whether that website "unabashedly announced" that it was a child pornography site, because the warrant searched every person who entered it, even first-time users. But Playpen contained a mix of legal and illegal content, as well as chat and message forums, and did not advertise itself as a child pornography site. *See* Ex. C, Screen Shot of Playpen Homepage. What's more, under the NIT warrant the government has claimed authority to conduct

100,000 or more searches anywhere in the world. So the search and seizure authority the Government claims in this case is truly unprecedented.

Second, the FBI intentionally or recklessly misled the issuing court about how the site appeared, and how the site could be found. Specifically, the warrant application alleged that the site's home page displayed purportedly lascivious pictures advertising the site's illegal content. But the FBI had seized control of the site before applying for the warrant and knew that these pictures had been removed. The application also made misleading claims about how the website could be found, casting opinions as facts. In truth, the government made no effort to find out how users were reaching the website, not even bothering to try a Google search. Therefore the defense requests a hearing, and eventual suppression, pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978).

Third, the warrant was unconstitutionally overbroad and failed to satisfy the Fourth Amendment's particularity requirement. Based on the government's interpretation, the warrant subjected any person that entered the website to secret electronic searches, even if they engaged in no illegal activity. This was unnecessarily overbroad, as the warrant could have and should have been tailored to apply to those who actually looked at illegal materials. In addition, the warrant

failed to satisfy the Fourth Amendment's requirement of particularity because it didn't specify where and who would be subject to search.

Fourth, the NIT warrant was an anticipatory warrant and the "triggering event" that would establish probable cause for searches did not occur. As explained in the warrant application, the triggering event was the act of (1) visiting Playpen's home page as described in the application, and then (2) entering the site. But the triggering event never occurred because the home page described in the application was gone by the time of the search. The home page as it actually appeared—both when the warrant was issued and the searches were executed—was different then described, and did not, as the FBI had claimed, show or suggest 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.

Fifth, the NIT warrant was issued in the Eastern District of Virginia (EDVA) and authorized searches of persons or property located in that district only. As a result, the search of Mr. Owens's Wisconsin computer exceeded the scope of the NIT warrant. The "good faith" exception also does not apply when a search is executed in a location that was not authorized by the underlying warrant.

In addition, in conjunction with this motion, the defense will submit a second motion to suppress explain that if the NIT warrant authorized searches outside the EDVA then the issuing magistrate judge lacked jurisdiction to issue it. According to the Government, the warrant authorized the FBI to search computers anywhere in the world. Such a warrant disregards the geographic limits of Rule 41(b), which in turn cabins the jurisdictional power of all federal magistrate judges under federal law. The NIT warrant was therefore void *ab initio*, as one judge in the District of Massachusetts has already determined. *See United States v. Levin*, No. CR 15-10271-WGY, 2016 WL 2596010 (D. Mass. May 5, 2016).

Finally, in conjunction with this motion, Mr. Owens is filing a separate motion to dismiss the indictment based on outrageous government conduct. The government executed all of its NIT searches, including the search of Mr. Owens's computer, after the FBI had seized control of Playpen on February 19, 2015. For roughly two weeks afterwards, the FBI allowed the site's more than 200,000 users to publish, distribute, and download massive amounts of child pornography from the site. This aspect of the investigation was not disclosed to the judge who issued the NIT warrant. And no statutory or other legal exemptions allow law enforcement to publicly disseminate child pornography. (Indeed, the law prevents

defense counsel from even temporarily possessing copies of such images, even though they will be used as evidence at trial.)

The FBI's actions were also grossly irresponsible because there was no need for agents to distribute child pornography in order to identify the people who were visiting Playpen. As a result, the Government has done far more to re-victimize the abused children found on the website than any defendants in this district who have been charged in this investigation. 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. It also raises issues regarding government 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. Under all these circumstances, suppression is not only appropriate but necessary to reinforce the rule of law.

Statement of Facts

A. The Playpen web site and the Tor network

On February 4, 2016, law enforcement agents executed a search warrant at

the home of Marcus Owens in Kenosha, Wisconsin, and physically seized (among other items) several electronic devices, including computers and hard drives. *See e.g.*, Docket Entry (Doc.) 1 at ¶5. This was the second search of Mr. Owens's home, the first having occurred on or about February 25, 2015, when the FBI used a form of malware called a "Network Investigative Technique" (NIT) to remotely search Mr. Owens's personal computer. *See* Ex. B at ¶27. This initial February 2015 search is the focus of Mr. Owens's Fourth Amendment challenges.

According to the discovery, the events leading to the two searches of Mr. Owens's home began in December 2014, when a "foreign law enforcement agency" contacted the FBI with a tip, claiming that it believed it had identified the IP address associated with the Playpen website. Ex. B at ¶28.

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 remains primarily funded by the U.S. Government. The network is designed to "protect users' privacy online." Ex. B at ¶ 8. In simple terms, people who want to use Tor can download a free browser and search engine (similar to Chrome or other Internet browsers) that provides added privacy protections. *Id.* at ¶7; *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 users' Internet Protocol (IP) addresses and other identifying information. *See* Ex. B at ¶¶ 6-9. Using the Tor network can be seen as the online equivalent of having an unlisted phone number and caller ID blocking.

Beyond enabling more privacy on the regular internet, the Tor network also can host individual websites. These websites are usually accessible only to those using Tor. Generally, everything about such a website is confidential: both the location of the server hosting the website and the users' information are protected by the Tor network.

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);[1] Virginia Heffernan, *Granting Anonymity*, N.Y. Times (Dec. 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.").[2] Millions of people now routinely use Tor to avoid targeted advertising, to protect their personal data from marketers and scammers, and to privately search for a wide variety of content. *See* Tor Metrics (last visited on May 29, 2016).[3]

In this case, due to an error in Playpen's connections with the Tor network, the site could be viewed intermittently through both Tor and a regular internet browser. *See, e.g.* Ex. A at ¶8, n. 4; Ex. B at ¶29, n.7. After receiving the tip from the unknown foreign government, the FBI found the server hosting the Playpen site, and then located the operator of the site. Ex. B at ¶¶28-30. The government raided his home in Naples, Florida, on February 19, 2015. *Id.*

B. The FBI's distribution of pornography from Playpen

On that same day, the FBI seized the physical computer server hosting

[1] Available at https://www.theguardian.com/technology/2014/jun/05/guardian-launches-securedrop-whistleblowers-documents.
[2] Available at http://www.nytimes.com/2010/12/19/magazine/19FOB-Medium-t.html?_r=0.
[3] Available at https://metrics.torproject.org/userstats-relay-country.html.

Playpen and moved it to a government facility in Virginia, where it maintained and operated the site until at least March 4, 2015. During this time the FBI continued to run the site like the prior operator, allowing new users to sign up, members to post child pornography, and any registered visitor to view and download such materials. It took no measures to block or limit the uploading, downloading, viewing, or redistribution of thousands of illicit pictures and videos.

As of February 20, 2015 the site had 158,094 members. Ex. B at ¶ 11. According to government information, it appears that approximately 56,000 new members joined the site after the FBI took it over and approximately 100,000 users visited the site during the two-week period that the FBI operated it. *See id.*; Ex. A at ¶12. This was a dramatic *increase* over the approximately 11,000 weekly visitors the site had before the FBI took it over. *See* Ex. 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," Ex. B. at ¶ 27, and also describes the site as a "website whose primary purpose is the advertisement and distribution of child

pornography." Ex. 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* Ex. D, Playpen Table of Contents (reflecting a "screenshot" of what users would see after logging in); Ex. B at ¶ 14.

In describing the "Places to be Searched," the warrant application oddly listed both "the computer server described below" and "the activating computers." The server was defined as the server hosting Playpen, which was under government control, and the activating computers as those "of any user or administrator who logs into [Playpen] by entering a username or password." Ex. B at Attachment A.

Of course, the actual targets were the "activating computers," not the server. This is because although the FBI had seized the Playpen server, that server did not contain any visitor data. Nor could that data be collected from third parties, such as AT&T or other internet providers, since the main purpose of the Tor browser and network is to privatize its users' identities. Ex. B at ¶¶ 8-9, 29.

Accordingly, deep into the warrant affidavit, the government explained that the FBI would use its NIT to search for data directly on the personal computers and other digital devices of Playpen's users. Ex. B at ¶¶33-34. This data included

users' 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 ¶34, 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 NIT gained access to personal computers without the owner or user's knowledge or consent, the NIT is a form of "malware." *See* Ex. E, Testimony of Dr. Christopher Soghoian, *United States v. Michaud*, Case No. 3:15-cr-5351 at 117 (W.D. Wa.).

Once the FBI had inserted the 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 a burglar disabling a building's 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 a house to find an address book or billing records. In this case, Mr. Owens's computer was located in his home when it was remotely searched and he had no knowledge that the search had even occurred until it was disclosed by the government in February 2016 (nearly a year later).

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.

Roughly 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, and it is unclear at this point how many of the 100,000 potential targets were actually searched.

As described above, 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 or broke the law. Visitors had to "log on" to access the site, but a 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. *Id.* at ¶14. The warrant application nevertheless sought authorization to search the computers of anyone who made it past the home page.

That application therefore focused on the appearance and content of the home page, as well as how the site could be found. 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." Ex. B at ¶ 12. The application did not claim that these pictures met 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.

This description of the home page was also wrong. The government has produced screen shots showing both how the site's home page appeared earlier in 2015, and how it appeared from February 19, 2015 until it was shut down. See Ex. C; Ex. F, Earlier Screenshot of Playpen Homepage. On that day, the home page did not contain any highly sexualized images of prepubescent girls. Instead it showed a picture of one fully clothed female, legs crossed. *See* Ex. C. While the female depicted on the home page appears young, the image is small and does not establish that she is a minor, let alone "prepubescent." *Id.* The FBI was aware that the site's description in the warrant application was wrong when it submitted that application. Nevertheless, the FBI did not disclose that information to the magistrate judge, and never submitted an amended or corrected affidavit.

The warrant application also made several statements describing how difficult it was to find Playpen, in effort to support the FBI's assertion that anyone who got to the site had to be looking for child pornography. But the statements supporting this conclusion have turned out to be either false or unverified assumptions. For example, the application states that a user had to use Tor to access Playpen. *See* Ex. B, Application ¶10. This was false, which the government knew at the time and which it later admitted explicitly. Ex. A at ¶8, n.4. Due to a misconfiguration, Playpen was intermittently accessible to regular internet users. *Id.* The application further states that "a user may not simply perform a Google search" for the name of a Tor website, like Playpen. Ex. B at ¶10. Instead, the affidavit contended that a person would have to communicate directly with an existing user, or get the site's address from "Internet postings" that would describe its content. *Id.* Yet the FBI had little-to-no foundation for these claims. No records show that it even tried to search for Playpen using Google, or any other search engine. *See* Ex. G, Letter from U.S. Attorney's Office to Defense Counsel (June 17, 2016). The FBI has records of Playpen's address being posted on only two other websites, and it failed to save screenshots of either one. *See* Ex. H, Letter from U.S. Attorney's Office to Defense Counsel (June 6, 2016) at 2. In truth, the FBI had little

idea of how a person might reach Playpen's website, and exhibited no apparent interest in finding that out.

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* Ex. B at ¶ 12. The affiant did not claim that this technical language suggests any criminality and explained, among other matters, 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. Ex. B at ¶ 27; Ex. D. Like the home page, the table of contents did not contain child pornography, 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. *See* Ex. D. But 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* Ex. B at ¶¶ 5(b) & 14; Ex. 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 further steps of selecting one of the sub-directories with a suggestive title; opening the sub-directory; and then scrolling 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).

Ex. B at 1 (emphasis added). Consistent with this statement, the warrant itself specifies the location to be searched as "property located in the Eastern District of Virginia." *Id.* at 2.

The warrant then refers to "Attachment A" to more particularly describe the "Place to be Searched" within that district. *Id.* at 3. Attachment A first lists the computer server operating the "TARGET WEBSITE," "which will be located at a government facility in the Eastern District of Virginia." *Id.* As noted, "Target Website" refers to the Playpen server that had already been seized. 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.* The attachment, however, does not identify any locations other than the Eastern District of Virginia, nor does it state that "activating computers" may be located outside the district or otherwise modify the explicit request on the application's first page that searches would apply 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. Owens's home computer

The FBI began searching computers on February 20, the same day the NIT warrant was granted. On or about February 25, 2015, FBI agents sent the NIT malware to a computer connected to someone with the username "tenderbittles"

and then seized data from it. Ex. A at ¶27.

In March 2015, the FBI used some of the data it had collected from that computer to prepare an administrative subpoena to Time Warner for related address information. *Id.* at ¶33. Time Warner responded with Mr. Owens's subscriber information, name and address. *Id.*

On February 4, 2015 at approximately 6 am, FBI and other law enforcement agents searched Mr. Owens's home pursuant to a second warrant issued by the Hon. Nancy Joseph the previous day. Pursuant to that warrant, agents seized several computers, hard drives, a cellular phone and other personal property. Mr. Owens was taken to a police station and interrogated by police. Then on February 9, 2016, this Court issued a criminal complaint charging Mr. Owens with receipt and possession of child pornography. He was arrested the following day at his place of work by the FBI, taken to an FBI office, and interrogated further.

Mr. Owens has never been previously charged with any criminal offense.

Argument

I. 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* Ex. B at ¶ 32 (seeking authority "to investigate *any* user or administrator who logs into" Playpen) (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 the NIT warrant application contained no specific information about the site's visitors and the application didn't include an expert "collector profile," probable cause depended on the contents of the home 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. *See United States v. Gourde*, 440 F.3d 1065, 1070 (9th Cir. 2006). While the warrant application claims 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* Ex. B at ¶6.

Ignoring the warrant application's inaccuracy for the moment, the only facts that would support the conclusion that the site was clearly 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." Ex. B at ¶ 12.

The affiant did not claim that these pictures met the definition of illegal "lascivious" images, and in fact they don't. *See United States v. Long*, 831 F. Supp. 582, 587 (W.D. Ky. 1993) (explaining that lascivious means "lewd"); *see generally 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"); *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"). Nor did the affiant include a copy of the home page with the warrant application so that the magistrate judge 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* Ex. C *with* Ex. I, Online images appearing in response to a Google search for "child models". And, without any (a) explicitly sexual pictures of children or (b) direct language to that effect, nothing on the home page shows that Playpen advertised or promoted itself as a child pornography site.

The rest of the facts in the affidavit about the site relate 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 subject is relevant, it adds little or nothing to the probable cause analysis because the government sought to search visitors as they were entering the site and before they could see what it contained. *Compare Gourde*, 440 F.3d at 1070 (affidavit established that the defendant had paid for a membership to site after having had an opportunity to view samples of the child pornography offered on the site); *United States v. Doan*, No. 05-CR-179-S, 2006 WL 5866677, at *5-*6 (W.D. Wis. Mar. 13, 2006) (same).

In short, given the facts alleged in the affidavit, 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 search is based on someone's mere accessing of a website, probable cause exists 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 associated with (1) a "men's lifestyle" magazine that was a knock-off of Playboy, *see* Ex. J, Playpen Covers; (2) numerous strip clubs around the country;[4] and (3)

[4] *See* http://playpenla.com/ (Los Angeles); http://www.yelp.com/biz/the-playpen-gentlemens-club-brooklyn (New York); https://foursquare.com/v/club-playpen/53e430b7498ed7b6e9b0cbdf (Portland).

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* Ex. C *with* Ex. K, Angel's Playpen Screenshot *and* Xtreme Playpen Homepage (last visited July 29, 2016).[5]

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." *Gourde*, 440 F.3d at 1067; *see Doan*, 2006 WL 5866677, at *5-*6. 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, 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").

Significantly, the site in *Gourde* also charged a membership fee and visitors

[5] Available at https://www.xtremeplaypen.com (this webpage contains explicit images, which is why no screenshot has been attached as an exhibit).

saw "images of nude and partially-dressed girls, some prepubescent" before they paid the fee and joined the site. *Gourde*, 440 F.3d at 1067; *see Doan*, 2006 WL 5866677, at *5-*6. 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 the defendant in *Gourde*, had indisputably viewed samples of child pornography and then chose not only to join

the site, but pay for a membership.

The NIT warrant application also 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. But the application does, however, claim that "numerous affirmative steps" were required for users to locate Playpen, and therefore it was "extremely unlikely that any user could simply stumble upon [it] without understanding its purpose and content." Ex. B at ¶ 10. Taken at face value, these statements are qualified guesses at best, relying on undefined terms like "numerous" and "unlikely." (They will be addressed more below in connection with Mr. Owens's request for *Franks* hearing.)

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. *Gourde,* 440 F.3d at 1072. Yet the NIT warrant application never linked the act of simply visiting Playpen's home page to specific offender characteristics. As a result, the warrant made no distinction between, (1) casual or "unwitting" visitors and "accidental browsers" and, (2) the subset of people actively seeking child pornography. Instead, both groups were authorized targets of the FBI's searches.

In short, the probable cause boundaries laid out in *Gourde*, *Martin*, *Doan* and elsewhere make sense, because the internet contains websites that cater to every imaginable taste and fetish. Many of these websites may be utterly repugnant, but most are 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 "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, "[a]lthough 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 "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, even taken at face value, the NIT warrant application was too slim of a reed on which to hang a sweeping authorization (as the Government interprets the warrant) to search 100,000 or more computers.

II. This 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, however, cannot be taken at face value. This is 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."

This doctrine applies to omissions, not just false statements. *See United States v. Glover*, 755 F.3d 811, 817 (7th Cir. 2014). It also includes cases where an affiant

makes false statements or omissions showing a "reckless disregard for the truth." *United States v. Williams*, 718 F.3d 644, 650 (7th Cir. 2013); *United States v. Meling*, 47 F.3d 1546, 1553 (9th Cir. 1995) ("recklessly fail[ing] to verify" material information). In addition, the doctrine may apply where warrants were "obtained by affidavits marred by omissions of facts required to prevent technically true statements in the affidavit from being misleading." *United States v. Kimberlin*, 805 F.2d 210, 252 (7th Cir. 1986) (citation and internal quotation marks omitted). In showing "reckless disregard," the court can consider the omissions or false statements themselves as circumstantial evidence of recklessness. *See United States v. Glover*, 755 F.3d 811, 820 (7th Cir. 2014). Once this threshold is met, the reviewing court considers whether the affidavit creates probable cause with its omissions filled and falsities "stricken." *United States v. Spears*, 673 F.3d 598, 604 (7th Cir. 2012) *see Wilson v. Russo*, 212 F.3d 781, 789 (3d Cir. 2000).

In this case, the false, misleading, and omitted statements were material. The descriptions of the home page and how the site could be found were pivotal components 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 seeking to search the computers of anyone who accessed the site, the Government contended that the site was not only "dedicated" to child pornography, but that this purpose would be apparent to anyone who reached and viewed its public home page. As a result, anyone who went even one step further would know what he or she was getting into.

The government tried to make this showing by including an incorrect description of the site, 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 United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1178 (9th Cir. 2010) ("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). Making matters worse, the affidavit contained inaccurate, conclusory statements about how the website could be found, which the government did almost nothing to verify. It didn't even conduct a simple Google search.

Taken as a whole, the misstatements and omissions in this case undermine

the already shaky case for probable cause. This case meets the standards for a *Franks* hearing, and the Court should order one held in this matter.

A. The government knowingly misportrayed the website's home page.

To begin, the government's knowingly included an incorrect description of the website in its application. As shown, the website included one small picture of young woman, sitting in a chair with her legs closed. Ex. C. It did not have, like the affidavit claimed, two pictures of obviously pre-pubescent girls with their legs spread. Ex. B, ¶12. This description was flatly wrong.

Since the government had the website under its control at the time, it knew exactly what the home page looked like when it applied for the warrant. But it didn't correct the error. Nor did it describe both the old and the new website. Instead, it chose to both submit the erroneous description *and* never tell the magistrate judge that the site had changed.

The affidavit also failed to mention how small the image is. *See* Ex. C. As the Court can see, the image is so small that one has difficulty making out details. It's also tucked away in a corner, and not a prominent feature of the home page. Comparing this to log on pages of adult pornography websites—where the images are front and center and clearly explicit—is striking. *Compare* Ex. D *with* Bangbros

Homepage.[6] One clearly advertises pornography. The other is ambiguous at best.

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* Ex. C. This feature is highlighted on the home page, prior to logging in, and printed in large, colorful capital letters near the center of the page. *Id.* Yet that fact is omitted in the application. 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 the site's visitors. *Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 870 (1997) ("there is no basis for qualifying the level of First Amendment scrutiny that should be applied' to online speech").

Even taken alone, the government's knowingly false description of the website merits a *Franks* hearing

B. The government's statements about how the website could be found were recklessly misleading at best, and omitted important information.

Given the relatively innocuous nature of the website's home page,

[6] Available at http://bangbros.com (this webpage may contain explicit images, so no screenshot has been attached as an exhibit).

particularly compared to adult pornography sites, another crucial argument in support of the warrant was how difficult it was to find the site. The affidavit claimed that because of this high degree of difficulty "it [is] extremely unlikely that any user" would get to the website without knowing "its purpose and content." Ex. B at ¶10. Discovery in this case has revealed that this statement was based on assumption and speculation. In short, the government didn't do its homework.

First, the affidavit misleadingly describes how difficult it is to find websites on the Tor network, going so far as to suggest that there is no such thing as a Tor equivalent of a Google search engine. These statements give the impression that anyone who found Playpen must have been determinedly seeking out child pornography. But this is simply not true.

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. *See, e.g.*, Ahmia, https://ahmia.fi/search; OnionLink, http://www.onion.link/. Using search terms for legal content, such as "sex chat" or "teen erotica," can readily lead Tor browsers to a variety of sites, some similar to Playpen. A person entering the term "Playpen" and "pictures" on one of these search engines may very well have found the site at issue. And given the use of the term "playpen"

with regard to legal adult images, such users could have had no intent to look for illegal pornography. *See generally United States v. Hill*, 459 F.3d 966, 970 (9th Cir. 2006) ("[N]ot 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").

Moreover, the affidavit misleadingly suggests that the government had looked for Playpen using conventional means, and found nothing. With that assumption, the idea that the website spread only by "word of mouth" between child pornography fans seems reasonable. *See* Ex. B at ¶10 (suggesting that users would learn of Playpen directly from existing users or on message boards that would describe its content). In truth, the government had almost no idea whether this was the case. That's because it never tried to find out.

Discovery has revealed no records of the government using any search engines (whether conventional or Tor-based) to look for Playpen. Ex. G. So the government had little idea how individuals were finding the site. In fact, the government knew of only two places on the entire internet where the site's address had been posted. Ex. H at 2. (As any statistician will say, two is far too small a

number to make conclusions about anything, especially something as complex as the internet. The government also failed to save "screenshots" of these two sites, therefore depriving the defense and this Court of the ability to evaluate them. *See id.*) None of this information was disclosed. Instead, the government suggested that it had found Playpen's website in many different places, where it was always identified as a child pornography site. Ex. B at ¶10 (using the term "for example"). That impression was misleading.

In reality, the government found the site's address in only two places on the entire internet. It didn't know (or probably care) how users were finding the site. So it filled in the affidavit with guesswork about how the site might be found, based on two websites and apparent ignorance about the Tor network.

C. The affidavit makes other misleading statements.

Further omissions and misleading statements tainted the affidavit. For example, the affiant claimed that "the entirety" of Playpen is "dedicated to child pornography." Ex. 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 based on facts showing that any visitor would know its illegal purpose when first logging in, given the point in time that the searches could be executed. But this description of

the site's content is false, as revealed by its table of contents. *See* Ex. D.

The application also fails to detail what specific sub-forums contained child pornography and what do not, and what percentage of posts on the site contain such materials. On the face of the affidavit, several of the most popular categories would appear to not contain such materials. *See* Ex. B. at ¶14 (noting 13,918 posts and 1,390 topics in the "General Discussion" forum).

Coupled with the absence of obvious "prepubescent" girls or even a clear indication from the home page that the site contains pornography, these facts 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." Ex. B at ¶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 many web sites that allow 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." Ex. B at ¶15. These same features are offered by Twitter and Facebook, among many other websites. Suggesting that they are somehow indicative of criminal behavior is similar to asserting that bank robbers "commonly" use cars. 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.

D. Without the incorrect and misleading statements and omissions, the warrant fails to establish probable cause.

Without the application's false description of the Playpen home page, its ungrounded assumptions about how the website could be found, its incorrect statements about Tor, and its misleading technical characterizations, the case for probable cause becomes too thin. After correcting or removing these assertions or omissions, the warrant fails to supply probable cause to search every person who entered the website, let alone a first time user. A simple look at the site's actual home page shows that. *Compare* Ex. C with *Gourde*, 440 F.3d at 1067 (describing

site's homepage). A *Franks* hearing is warranted in this case.

III. The NIT warrant was overbroad and lacked particularity.

The NIT warrant application's probable cause shortcomings are worsened by the extraordinary scale of the search authorization that the Government is claiming and by the lack of specificity in its request.

A. The warrant could have, but failed to, exclude individuals who broke no laws, and was thus overbroad.

Federal law explains that when it comes to the question of whether a warrant is overbroad, there is a direct relationship between the scope of the search authorized and the extent to which probable cause has been established; the broader the search, the more extensive the showing of probable cause must be. *See 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 asked for (and received) an unprecedentedly sweeping warrant. Unlike a typical search warrant that relies on facts about 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, 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").[7]

As a result, the NIT warrant could 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. Or since the FBI could send its malware to anyone who logged into the site, the warrant could have required the FBI to target only those who "clicked" on particular sub-directories with illegal content or particular pictures or links in those sub-directories. Indeed,

[7] Available at https://www.wired.com/2014/08/operation_torpedo/.

in a footnote, the affiant suggested that the FBI might do exactly that, yet the warrant does nothing to particularize or narrow the set of visitors who would be subjected to searches. Ex. B at ¶32, n. 8. And this would have been an appropriate line to draw given all that was known about the site.

It is this type of narrowing of computer searches, or search protocols, that circuit courts have admonished judges to impose when issuing warrants to seize electronic data. *See Comprehensive Drug Testing*, 621 F.3d at 1172, 1177 (disapproving of "deliberate overreaching" by the Government in seizing electronic data, and requiring judges to exercise "greater vigilance" when approving computer search warrant applications). The request must be as particular as the circumstances reasonably permit. *United States v. Bentley*, 825 F.2d 1104, 1110 (7th Cir. 1987) ("The description must be as particular as the circumstances reasonably permit. So if the fraud infects only one part of the business, the warrant must be so limited . . . .").

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); *see also United States v. Pritchard*, 745 F.2d 1112, 1122

(7th Cir. 1984). So a warrant must give clear and legal (not overbroad) instructions to police. *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 702-03 (9th Cir. 2009); *Pritchard*, 745 F.2d at 1122 (warrants that are worded too vaguely may be held as overbroad); *see also 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 who may have done and intended to do nothing illegal, 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 Green Bay, Wisconsin, and many other medium-sized 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 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).

B. The warrant also failed to meet the Fourth Amendment's particularity requirement.

Under the Fourth Amendment, a warrant must "particularly describe" the place to be searched." U.S. Const. Amend. IV. Warrants that do not specifically describe the place to be searched and the items to be seized are invalid. *Groh v. Ramirez*, 540 U.S. 551, 559 (2004) (explaining that "the presumptive rule against warrantless searches applies with equal force to searches whose only defect is a lack of particularity in the warrant"). This rule must be met by the warrant itself. A warrant affidavit will not save an insufficiently particular warrant if the affidavit is not incorporated. *See id.* at 554.

In this case the NIT warrant fails the particularity requirement because it doesn't describe the place to be searched. No reasonable person, from reading the warrant, would know exactly where the searches would be occurring. No address or location is listed in the NIT warrant, let alone in the unincorporated NIT

warrant application. In the blank where the government or court is supposed to provide a description of the place or person to be searched, the warrant refers to "Attachment A." *See* Ex. B at 1. And Attachment A confusingly describes both the "TARGET WEBSITE" (which wasn't actually searched at all) and then unnamed and unnumbered "activating computers." *Id.* at Attachment A. No information is given about what these "activating computers" are, who is operating them, or where they are located.

The government will undoubtedly state that it couldn't answer these questions, so it couldn't provide that information--that was the point of the warrant. This answer might be acceptable, but for the fact that the actual warrant states that the search location is in the EDVA. So to the extent that the warrant is at all particular, it is particular to that district. Suppression should be required for all information gathered outside that district. *See, e.g.*, See *United States v. Sedaghaty*, 728 F.3d 885, 913 (9th Cir. 2013) (though affidavit could be read as describing a broad category of items, "the language of the warrant controls" and any evidence exceeding the authorization in the actual warrant should be suppressed).

IV. The NIT Warrant was an anticipatory warrant and the "triggering event" for the computer searches never occurred.

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 Ex. 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 Seventh Circuit has explained, "conditions precedent to the execution of an anticipatory warrant are integral to its validity." *United States v. Dennis*, 115 F.3d 524, 528 (7th Cir. 1997). If the conditions are not met at the time of the actual search, then the search is invalid. *See id.*; *United States v. Vesikuru*, 314 F.3d 1116, 1119 (9th Cir. 2002) ("The 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.").

In this case, the warrant allowed searches of anyone who signed into Playpen (the triggering event) only if the site continued to "unabashedly announce" that it was dedicated to child pornography. Assuming that the warrant application's description of the Playpen home page created probable cause that anyone who entered the site was a legitimate search target, that conclusion was

undermined when that description proved to be wrong.

Because the website had changed, the triggering event described in that warrant application could not, and did not, occur. And since the triggering event did not occur, any searches based on the NIT warrant 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 anyway. 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 relied on to "trigger" the searches no longer existed by the time those searches occurred. As a result, when the Government proceeded with the NIT searches anyway, it exceeded the scope of the warrant, and suppression is required. *See United States v. Elst*, 579 F.3d 740, 744 (7th Cir. 2009) (probable cause depends on "if the triggering condition occurs"); *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.").

V. The NIT Search of Mr. Owens's Washington Computer was Not Authorized by the Warrant.

Finally, 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 search warrant didn't grant the FBI the power to search a computer in Wisconsin.

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 . . . .

Ex. B at Attachment B (emphasis added). Consistent with this sworn statement, the NIT warrant itself authorizes searches of "person or property located in the Eastern District of Virginia." Ex. B at 2.

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 Wisconsin (Mr. Owens'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 EDVA. This attachment does not alter the specific location stated on the face of the warrant. 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.

The Government may argue that the magistrate judge authorized it to search computers anywhere 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. Ex. B at ¶46(a). But this argument is

unavailing. Again, the application was not incorporated into the warrant itself. And even assuming that such a passing reference was enough to apprise the magistrate judge that the FBI intended to search computers anywhere in the world, it does not change the fact that she issued 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."). Indeed, as noted in Mr. Owens's other motion to suppress, reading the warrant as authorizing searches in the EDVA only is the single way that the warrant could comply Rule 41(b).

Accordingly, the warrant and attachment authorize searches of "activating computers" wherever they may be located *in the EDVA*. Nothing within the four corners of the warrant 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. *See United States v. Sedaghaty*, 728 F.3d 885, 913 (9th Cir. 2013) ("the language of the warrant controls" and suppression is required for any evidence

that exceeds the scope of the authorization in the warrant itself). At the very least, the warrant is ambiguous as to where searches are authorized. And under the law, a facially ambiguous warrant it is invalid and cannot legally be executed. *Jones v. Wilhelm*, 425 F.3d 455, 463 (7th Cir. 2005) ("Where a warrant is open to more than one interpretation, the warrant is ambiguous and invalid on its face and, therefore, cannot be legally executed by a person who knows the warrant to be ambiguous.").

Conclusion

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

Moreover, even if there had been probable cause, the warrant was overbroad and lacked particularity, relied on an anticipatory condition that never occurred, and the magistrate judge who issued the warrant expressly limited the geographic scope of her search authorization to the Eastern District of Virginia. These collective errors require suppression. Accordingly, the Court should

suppress all evidence seized during the February 2015, search of Mr. Owens's home computer and all fruits of that search.

Dated at Milwaukee, Wisconsin this 1st day of August, 2016.

Respectfully submitted,

/s/ Anderson M. Gansner

Anderson M. Gansner, Bar No. 1082334
FEDERAL DEFENDER SERVICES
OF WISCONSIN, INC.
517 E. Wisconsin Avenue, Room 182
Milwaukee, Wisconsin 53202
Telephone: 414-221-9900
Fax: 414-221-9901
E-mail: anderson_gansner@fd.org

Counsel for Defendant,
Marcus A. Owens