JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. DAVID TIPPENS, Defendant.	No. CR16-5110RJB **MOTION AND MEMORANDUM IN SUPPORT OF MOTION TO SUPPRESS EVIDENCE** ***[Oral Argument Requested]*** **NOTED: September 2, 2016**
UNITED STATES OF AMERICA, Plaintiff, v. GERALD LESAN, Defendant.	No. CR15-387RJB **MOTION AND MEMORANDUM IN SUPPORT OF MOTION TO SUPPRESS EVIDENCE** ***[Oral Argument Requested]*** **NOTED: September 2, 2016**
UNITED STATES OF AMERICA, Plaintiff, v. BRUCE LORENTE, Defendant.	No. CR15-274RJB **MOTION AND MEMORANDUM IN SUPPORT OF MOTION TO SUPPRESS EVIDENCE** ***[Oral Argument Requested]*** **NOTED: September 2, 2016**

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

I. INTRODUCTION

David Tippens, through his attorney Colin Fieman, respectfully moves the Court pursuant to Fed. R. Crim. P. 12(b)(3)(c) for an order suppressing all evidence, and the fruits of all evidence, seized from Mr. Tippens's home computer by the FBI on or about February 26 and 28, 2015.

Gerald Lesan, through his attorney Robert Goldsmith, joins this motion and respectfully seeks an order suppressing all evidence, and the fruits of all evidence, seized from Mr. Lesan's home computer by the FBI on or about March 5, 2015.

Bruce Lorente, through his attorney Mohammad Hamoudi, also joins this motion and respectfully seeks an order suppressing all evidence, and the fruits of all evidence, seized from Mr. Lorente's home computer by the FBI on or about February 23 and 24, 2015.

The evidence, consisting of "Media Access Card" (MAC) addresses, "Internet Protocol" (IP) addresses, and other electronic data, was seized by the Government with "Network Investigative Technique" (NIT) malware that was inserted by FBI agents located in Virginia onto all three defendants' computers in Washington.

While the Court previously denied a motion to suppress in the related case of *United States v. Michaud*, No. 3:15–CR–05351–RJB, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016) (hereinafter "*Michaud* Order"), the Court should rule differently in this case for several reasons.

First, in *Michaud*, the defense did not argue (and the Court therefore did not consider) that the NIT search warrant issued in the Eastern District of Virginia (EDVA) that purportedly authorized the search of the defendants' computers was *void ab initio* because it was issued in violation of the Federal Magistrate's Act, 28 U.S.C. § 636. *See* § III-A, *supra* at 11.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Second, the Court has previously found that the NIT warrant violated Fed. R. Crim. P. 41. *See* 2016 WL 337263 at *6. However, the Court decided that suppression was not required because the violation was "technical." *Id.* We assert that under the controlling Ninth Circuit authority this violation was fundamental (or "structural") because it was jurisdictional and therefore suppression is required. Further, suppression is required on the independent ground that the Government deliberately violated Rule 41. *See* § III-B, *supra* at 15.

Third, in deciding there was no reasonable expectation of privacy in the assigned IP address, the *Michaud* Order did not take into account the MAC address along with other items obtained in the NIT search. As well, we assert that this Court erroneously ruled that the Government did not infringe on a legitimate expectation of privacy with its NIT searches, a conclusion that cannot be reconciled with the relevant Supreme Court precedents. *See* §III-B(2), *supra* at 17.

Fourth, the Court in the *Michaud* Order, incorporated a reference in the warrant application to broaden the search area from the Eastern District of Virginia (as stated on the face sheets of both the warrant and application) to the entire world. 2016 WL 337263 at *4. This incorporation and expansion of the scope of the warrant contravenes Ninth Circuit precedent. *See* § III-C, *supra* at 22.

Finally, this Court should make a fresh assessment of probable cause for the NIT searches (an issue it did not address in detail in the *Michaud* Order) and, relatedly, order a *Franks* hearing. New testimony by the lead FBI Special Agent for "Operation Pacifier," Daniel Alfin, has confirmed that he personally contributed most of the information in the NIT warrant application and that he was aware of material changes to the "Playpen" home page. As a result, the FBI recklessly or deliberately presented false information about Playpen in the warrant application. *See* § III-D, *supra* at 25, and § III-E at 31.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

The Court is already familiar with the facts related to "Operation Pacifier" and the Government's use of a NIT. Accordingly, a relatively brief summary of the facts is included here.

II. STATEMENT OF FACTS

A. The Residential and NIT Warrants

On February 11, 2016, FBI agents assisted by local law enforcement executed a search warrant at Mr. Tippens's home in University Place, Washington. Mr. Tippens is 46 years old and an active duty solider. He has no criminal history. The search was conducted pursuant to a warrant issued by the Hon. Karen Strombom on February 9, 2016. Exh. C (the local Tippens warrant and supporting application).

On November 9, 2016, FBI agents assisted by local law enforcement executed a search warrant at Mr. Lesan's home in Everett, Washington. Mr. Lesan is now 49 years old and had been employed at Premera Health Insurance for 13 years in network technology. He was terminated after this case was filed and is currently studying to be a welder and looking for full time employment. He has no criminal history. The search was conducted pursuant to warrants issued by the Hon. Dean Brett on November 3, 2015. Exh. D (the local Lesan warrants and supporting application).

On July 28, 2015, law enforcement agents executed a search warrant at the home of Bruce Lorente in Seattle, Washington, and seized (among other items) several personal computers. Exh. E. (the local Lorente warrants and supporting applications). Mr. Lorente, who is now in custody, was receiving disability payments. He continues to suffer from serious medical conditions. Mr. Lorente has no criminal history except a burglary conviction from 1978, when he was 19 years old.

The searches of the defendants' homes pursuant to the locally issued warrants were the second searches of their homes. The first searches occurred between February

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

20 and March 5, 2015, when the FBI used a "Network Investigative Technique" (NIT) malware to conduct remote searches of the defendants' personal computers.

As set forth in the local warrant applications, the events leading to the search of the defendants' homes began on February 19, 2015, when the FBI took control of the "Playpen" website and moved it to a government server in Virginia. *See* Exh. A (NIT warrant application) at ¶ 30.[1] This seizure occurred as part of an FBI operation called "Operation Pacifier" that ultimately targeted over 100,000 computers around the world, including Europe and Australia.

On February 20, 2015, the FBI submitted the NIT warrant application to Magistrate Judge Theresa Carroll Buchanan in the Eastern District of Virginia. This application sought authorization to use the NIT to search "activating computers," which are the computers "of any user or administrator who logs into [Playpen] by entering a username and password." Exh. B at Bates 136 ("Attachment A").

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. A (NIT warrant application) at Bates 134 (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. B at Bates 135.

The warrant did not incorporate the warrant application by reference, nor was the application physically attached to the warrant.

---

[1] The attached copy of the NIT warrant and its supporting application were disclosed in the *Michaud* case and is marked accordingly. The Government has not separately provided copies of the warrant and application as part of the discovery in each of the instant cases, but the same NIT warrant and application was used in all of them.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

The warrant application further stated that the NIT would seize information from the target computers, including their MAC addresses. Exh. A at Bates 137 ("Attachment B"). MAC addresses are unique identifiers individually assigned to computers and are not transmitted to internet service providers as part of email communications, or otherwise routinely disclosed to third parties. *See* exh. B at ¶ 34(g). As Agent Alfin recently testified in an Arkansas NIT case, even if an IP address changes, "the MAC address on, say, your laptop will not. That is essentially hardwired into that device. It is a unique identifier." Exh. K (*United States v. Jean*, CR15-50087TLB, June 13, 2016, Hearing Transcript) at 44.

Once the FBI had inserted a NIT onto a computer it did several things to seize data. First, the NIT altered or overrode a computer's security settings, so that the NIT could install itself on the targeted computer, similar to disabling a home's burglar alarm system before climbing through a window. Exh. F (January 22, 2016, hearing transcript) 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. At the time of the NIT searches in this case, all of the defendants' computers were located in their homes and they had no knowledge that the searches had even occurred until after they were arrested and charged, more than a year later.

Finally, the NIT overrode the user's Tor browser protections and forced the computer to send 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.

In addition to MAC addresses, the Government also used the NIT to seize the Internet Protocol (IP) addresses of target computers. Exh. B at Bates 137. The NIT

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

warrant application expressly states that there was no way for the FBI to obtain IP addresses from Internet Service Providers or other third parties because Tor is designed to keep IPs private. Exh. A at ¶ 8; *see also id*. at ¶¶ 9, 29. Agent Alfin has also recently conceded during testimony in another NIT case that, without the NIT, it would have been "impossible" for the FBI to obtain any IP addresses. Exh. K at 57.

Moreover, the Government has given conflicting accounts of exactly how it seized IP addresses. In *Michaud*, the Government claimed that IP addresses were seized by the NIT from the target computers themselves. *See*, *e.g.*, exh. A at Bates 137 (stating that the items to be seized "from any 'activating' computer" includes the computer's "actual IP address, and the date and time that the NIT determines what that IP address is"); *Michaud*, Dkt. 74 at 7 (Govt. Response to Motion to Compel) (stating that the information seized *from* Mr. Michaud's computer included his IP address).

Subsequently, during testimony in a Virginia NIT case, Agent Alfin testified that IP addresses were somehow seized in transit over the regular Internet after the NIT forced target computers to send data to the FBI. Exh. L (*United States v. Matish*, CR16-00016HCM, May 19, 2016 Hearing Transcript excerpt) at 26. Alfin has also testified that this data was unencrypted and, contrary to earlier declarations, vulnerable to corruption. Exh. K at 91-92. To this day, it is unclear how the NIT actually worked; what changes it made to the defendants' computers and data; or what vulnerabilities to additional hacking and third party control it created. *See* Defendants' Motion to Exclude (filed in conjunction with this motion).

B. The NIT Warrant Application's Probable Cause Showing

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 merely passed through Playpen's home page.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

The application describes the home page as containing a banner with "two images depicting partially clothed prepubescent girls with their legs spread apart." Exh. A at ¶ 12. This description of the home page is not accurate and the FBI knew that it was not accurate when it applied for the NIT warrant.

The home page, as it actually appeared from February 19, 2015 (the day before the warrant application) until the site was shut down, does not display any child pornography. Instead, the home page showed a picture of a fully clothed female, legs crossed. Exh. G. 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, evidence and testimony related to the February 19 search of the original site operator's Florida home establishes that the FBI was aware of the site's actual appearance on that date. Agent Alfin has now testified (at least twice) that he saw the changes that had been made to the home page before the NIT warrant application was submitted and that he "provided the bulk of the information that went into that warrant." Exh. K at 81. Nevertheless, the FBI did not disclose this information in the application presented to Magistrate Judge Buchanan the following day.

The FBI began "deploying" its NIT on February 20, the same day the NIT warrant was issued. During this time, the FBI continued to post child pornography on Playpen; it has since confirmed that it had at least 22,000 pictures, videos and links to pictures and videos on its website. A reasonable estimate of the actual scale of the FBI's distribution, given the available facts, is somewhere around 1,000,000 picture and video distributions. *See* Defendants' Motion to Dismiss Indictment.

The FBI also increased the traffic to its site from approximately 11,000 visitors per week prior to its seizure to approximately 50,000 per week after the seizure, with approximately one million total logins while the site was under FBI control. Exh. A at

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

¶ 19; *Michaud*, dkt. 109 (Govt. response to order compelling discovery) at 4. The Government has declined to explain how it managed to increase the visitor traffic to its site so rapidly and exponentially. However, it is undisputed that, for at least a two week period, the FBI became the world's largest distributor of child pornography on the Tor network.

C. The Residential Warrants' Probable Cause Showings

1. The Search of Mr. Tippens's Home

According to the Tippens residential warrant application, on February 26 and 28 a Playpen visitor with the user name "candygirl123" viewed pornography on the site and on one or both of those occasions the FBI sent its NIT to the user's computer. Based on the data seized from that computer (which was located in University Place, Washington), the FBI was able to determine that Time Warner was the service provider for it. In March, 2015, the FBI sent a subpoena to Time Warner for the physical address associated with the user's account. Time Warner responded with Mr. Tippens's subscriber information, including telephone number and address.

On February 11, 2016, FBI agents executed the residential warrant at Mr. Tippens's home and seized, among other items, his personal computer. Mr. Tippens cooperated with the agents and, according to the discovery, admitting viewing child pornography. There is no allegation that he was involved in producing or distributing illicit pictures, or that he has been involved in any type of "hands on" offense.

2. The Search of Mr. Lesan's Home

According to the Lesan residential warrant application, on March 5, 2015, "RandomUser67" logged into the website for .71 hours, browsed the website and accessed a post with links to a video and comments such as "she was my first pedo

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

obsession." [2] The FBI inserted an NIT onto his computer and seized an IP address and other data from it. The affidavit goes on to state that on March 5, 2015, "RandomUser67" accessed two additional posts with links to three pictures of child pornography, but indicates that the user's IP address "was not collected." Exh. D at 17.

Based on the data seized from that computer (which was located in Everett, Washington, at the time), the FBI was able to determine that Frontier Communications was the service provider for it. In March, 2015, the FBI sent a subpoena to Frontier Communications for the physical address associated with the user's account. Frontier Communications responded with Mr. Lesan's subscriber information.

On November 9, 2015, FBI agents executed the residential warrant at Mr. Lesan's home and seized, among other items, his personal computers, cell phones and cameras. This second search led to the charges before this Court.

3. The Search of Mr. Lorente's Home

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. Lorente's subscriber information, name and address.

On July 28, 2015, FBI and other law enforcement agents searched Mr. Lorente's home pursuant to a second warrant issued by the Hon. Mary Alice Theiler the previous

[2] The Affidavit in Support of Application for Search Warrant in Lesan's case, exh. D at 10, reads: "The website operated in Newington, Virginia, from February 20, 2015 until March 4, 2015, at which time 'Website A' ceased to operate." It is not clear from government explanations of time differences how Lesan's alleged March 5 access to Playpen came within the strict authorization period, which ended on March 4, 2015.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

day. Pursuant to that warrant agents seized several computers, hard drives, a cellular phone and other personal property. The police also seized a sex doll with a child's face.

Mr. Lorente was then detained and interrogated over several hours, during which he agreed to take a polygraph test. During this interrogation Mr. Lorente, who is 58 years old, reported that he has been treated for severe depression since 2011 and allegedly admitted possessing child pornography and having had sexual contact with two of his sisters when he was teenager. Mr. Lorente 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 "Void Ab Initio" Because it Violated the Federal Magistrate's Act and was Issued Without Jurisdiction.

The Government maintains that the NIT warrant, issued in Virginia, authorized it to search an unlimited number of computers anywhere in the world. The defendants' computers were all located in Washington at the time the Government used the NIT to remotely search them.

The NIT warrant was issued by a U.S. Magistrate Judge, whose powers are defined and limited by 28 U.S.C. § 636 (the Federal Magistrate's Act). The Act both establishes and limits the powers of a Magistrate Judge; it expressly provides that their jurisdiction extends only "within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law." 28 U.S.C. § 636(a). Consistent with this law, the Ninth Circuit has stated that "[f]ederal magistrates are creatures of statute, and so is their jurisdiction. We cannot augment it; we cannot ask them to do something Congress

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

has not authorized them to do." *United States v. Colacurcio*, 84 F.3d 326, 328 (9th Cir. 1996) (citation omitted).[3]

Since Magistrate Judges are not "Article III" judges under the U.S. Constitution, the Magistrate Judge who issued the NIT warrant had no more power to authorize searches outside the EDVA than did, for example, her law clerk or a U.S. Marshall. *See Dawson v. Marshall*, 561 F.3d 930, 932 (9th Cir. 2009) ("Section 636 outlines the jurisdiction, powers, and temporary assignments of magistrate judges."); *see also United States v. Luk*, 859 F.2d 667, 672 (9th Cir.1988) (noting that "warrants issued by unauthorized persons" defeat the purpose of "requiring an appropriate federal or state judge or magistrate to review the reasonableness and probable cause basis of a search warrant"); *United States v. Glover*, 736 F.3d 509, 514-15 (D.C. Cir. 2013) (explaining that a warrant issued in "blatant disregard" of a judge's territorial jurisdiction cannot be excused as a mere "technical" defect); *United States v. Scott*, 260 F.3d 512, 515 (6th Cir. 2001) (holding that "when a warrant is signed by someone who lacks the legal authority necessary to issue search warrants, the warrant is void *ab initio*"), *overruled on other grounds*, *United States v. Master*, 614 F.3d 236, 242 (6th Cir. 2010).

The limited, statutory basis of a Magistrate Judge's powers was not raised or briefed in the *Michaud* case. Accordingly, the Court has not had an opportunity to rule on this issue.[4]

---

[3] Congress intended that the magistrates "cull from the ever-growing workload of the United States district judge matters that are more desirably performed by a lower tier of judicial officer." H. Rep. Report No. 1629, 90th Cong., 2d Sess. 12 (1968), reprinted in 1968 U.S. Code Cong. & Admin. News 4254, 4255. *See* 12 Fed. Prac. & Proc. Civ. § 3066 (2d ed.).

[4] Notably, in *Michaud*, the Court asked the parties to address whether the validity of the warrant was affected by the fact that it had been issued by a Magistrate Judge rather than a District Court Judge. *See Michaud*, dkt. 125 (January 20, 2016, Order Regarding Hearings). At the time, the defense focused on the requirements of Fed. R. Crim. P. 41

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Moreover, four months after the *Michaud* suppression ruling, another court had an opportunity to rule on the jurisdictional implications of the Magistrate's Act. *United States v. Levin*, No. 15–10271, __ F. Supp. 3d __, 2016 WL 2596010 at *7 (D. Mass. May 5, 2016). *Levin* provides a compelling analysis of the jurisdictional violations at the heart of the NIT warrant.

First, the court concluded, just as this Court did in *Michaud*, that the NIT searches took place in the districts where the defendants' computers were located. *Levin*, 2016 WL 2596010 at *5 (citing *Michaud*, 2016 WL 337263 at *6). The Government no longer disputes that the NIT searches occurred in those districts. *Compare, e.g.*, *Michaud*, dkt. 47 (Govt. Response to Motion to Suppress) at 11.

Second, *Levin* also decided, just as this Court did in *Michaud*, that because of the worldwide scope of the ostensible search authorization, the warrant was not authorized by any of the provisions of Rule 41. *Levin*, 2016 WL 2596010 at *5-6; *Michaud*, 2016 WL 337263 at *5-6.

Third, and most importantly, the *Levin* court granted suppression because the "Federal Magistrates Act did not authorize the magistrate judge to issue the NIT Warrant here." 2016 WL 2596010 at *4, 11, citing *Scott*, *supra*; *see also United States v. Neering*, 194 F. Supp. 2d 620, 627-28 (E.D. Mich. 2002) (warrant issued by a judge who was not properly appointed was void and good faith exception did not apply.)

Elaborating on this conclusion, the *Levin* court stated, "Because a warrant that was void at the outset is akin to no warrant at all, cases involving the application of the good-faith exception to evidence seized pursuant to a warrantless search are especially

---

and both parties erroneously maintained that it would have made no difference if the warrant had been issued by a District Court Judge. *See Michaud*, Dkt. 127 at 3 (Response to Court's Enumerated Questions); January 22, 2016 Hearing Transcript at 151-52.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

instructive." *Id.* (citing *United States v. Curzi*, 867 F.2d 36 (1st Cir.1989)); *see also, United States v. Winsor*, 846 F.2d 1569, 1579 (9th Cir.1988) (declining to extend *Leon*'s good faith exception to searches not conducted in reliance on a warrant or a statute).

The *Levin* court then explained, "To hold that the good-faith exception is applicable here would collapse the distinction between a voidable and a void warrant. But this distinction is meaningful: the former involves 'judicial error,' such as 'misjudging the sufficiency of the evidence or the warrant application's fulfillment of the statutory requirements[,]' while the latter involves 'judicial authority,' i.e., a judge 'act[ing] outside of the law, outside of the authority granted to judges in the first place.'" *Id*. (citation omitted; brackets in *Levin*); *cf. Allen v. Meyer*, 755 F.3d 866, 867 (9th Cir. 2014) ("Because the magistrate judge entered judgment [outside the limits of § 636], the judgment was invalid.").

The *Levin* court went further, and held that even if a balancing were called for, it would still suppress. Addressing what the affiant, "a veteran FBI agent with 19 years of federal law enforcement experience," should have known given the plain language of the Federal Magistrate's Act and Fed. R. Crim. P. 41, the court concluded that "it was not objectively reasonable for law enforcement" to believe that the warrant had been properly issued. 2016 WL 2596010 at *13 (quoting the Government's pleadings). While at least one district court, in Virginia, has disagreed with *Levin*'s analysis of the Federal Magistrate's Act, the *Levin*'s court conclusions flow directly from the plain language of the Act and the relevant (albeit limited) case law. *See United States v. Matish*, 2016 WL 3545776 (E.D. Va. June 23, 2016).

Finally, another case decided after this Court ruled on the *Michaud* suppression motions is instructive on the jurisdictional issue. In *United States v. Barber*, __ F. Supp. 3d __, 2016 WL 1660534 (D. Kan. 2016), the court addressed a warrant that was

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

issued by a Maryland Magistrate Judge for digital evidence in California. The court concluded, just as the *Levin* court did, that the judge had no authority to issue the warrant and "warrants issued without jurisdiction are void from their inception[.]" 2016 WL 1660534 at *4. It next held that "[a] warrant that is void from its inception is no warrant at all." *Id.* The court also determined that "the good faith exception applies only to evidence seized under a once-valid warrant that was subsequently invalidated—not evidence seized pursuant to a warrant that was void at its inception." *Id.* at *4.

This Court should rule the same as the *Levin* and *Barber* courts did as to the Magistrate Judge's lack of jurisdiction under 28 U.S.C. § 636 and grant suppression in this case.

B. Suppression is Also the Required Remedy for the Rule 41 Violations.

1. There was prejudice because the violation was fundamental

In *Michaud*, the court concluded that the NIT warrant violated Rule 41, but declined to order suppression. The Court recognized that, under the controlling Ninth Circuit precedents, suppression is required if a defendant is prejudiced "in the sense that the search would not have occurred. . . if the rule had been followed." *Michaud*, 2016 WL 337262 at *6, quoting *United States v. Weiland*, 420 F.3d 1062, 1071 (9th Cir 2005) (ellipsis in *Michaud*). However, the Court interpreted this rule to mean that "courts should consider whether the evidence obtained from a warrant that violates Rule 41(b) could have been available by other lawful means, and if so, the defendant did not suffer prejudice." *Id*. (citing *United States v. Vasser*, 648 F.2d 507, 511 (9th Cir. 1980). The movants respectfully suggest that the Court erred in *Michaud* and should rule otherwise here, for the following reasons.

First, the threshold question for determining prejudice, as stated in *Weiland*, is whether *the search at issue* would still have occurred without the Rule violation. None of the relevant cases, including *Vasser*, hold that a defendant does not suffer prejudice

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

for Rule 41 purposes if the evidence that is seized during the search might have been obtainable through other means. And, in any event it, would have been impossible for the FBI to collect IP addresses without the NIT searches.

More basically, issuing a warrant for locations that are not authorized by Rule 41 is a fundamental "jurisdictional flaw" that cannot be excused as a "technical defect." *United States v. Glover*, 736 F.3d 509, 515 (D.C. Cir. 2014); *see also Levin*, 2016 WL 2596010 at *7-8; *United States v. Arterbury*, 2016 U.S. Dist. LEXIS 67091, *30, 35 (N.D. Okla. 2016) ("The NIT Warrant clearly did not comport with Fed. R. Crim. P. 41(b), and, therefore, was invalid *ab initio*. Arterbury was prejudiced by issuance of the NIT Warrant and the Court finds no basis for application of the good faith exception to the exclusionary rule."); *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).

Here, the three defendants were indisputably "prejudiced," as that term is applied in *Weiland*, because the search of their computers would not have occurred if the NIT warrant had complied with Rule 41(b). *Compare United States v. Williamson*, 439 F.3d 1125 (9th Cir. 2006) (technical failure of not providing a copy of the warrant to the person on the premises does not require suppression).

Second, the Court's conclusion that the IP addresses of NIT targets could eventually have been discovered from third parties has no basis in the record and is contradicted by both the NIT warrant application itself and later testimony by Agent Alfin. *See Michaud*, 2016 WL 337262 at *7. The application states that "traditional IP identification techniques are not viable" and "[t]here is no practical way to trace the user's actual IP back" through the Tor network. Exh. B at ¶ 8; *see also id*. at ¶¶ 9, 29.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Likewise, Agent Alfin has recently testified that "the NIT was the only investigative method available to the FBI that would allow us to identify [Playpen] users" and it would have been "impossible" for the FBI to obtain IP addresses without the NIT. Exh. K at 37 and 57.

Arterbury, an Oklahoma NIT case, addressed this point in some detail before granting suppression. "Were the IP address obtained from a third-party, the Court might have sympathy for [the Government's] position. However, here the IP address was obtained through use of computer malware that entered Defendant's home, seized his computer and directed it to provide information that the Macfarlane affidavit states was unobtainable in any other way. Defendant endeavored to maintain the confidentiality of his IP address, and had an expectation that the Government would not surreptitiously enter his home and secure the information from his computer." 2016 U.S. Dist. LEXIS 67091 at *35.

The general expectation of privacy that attaches to Tor was recently confirmed by the Government itself, in remarks that Ovie Carroll, a cybersecurity specialist with the Department of Justice, made at a recent judicial conference. *See Lorente* July 28, 2016, Transcript of Hearing on Motion to Withdraw Pleas at 3.

Plainly, the FBI's inability to obtain IP addresses from third parties or otherwise without trespassing on the defendants' home computers was the reason for doing NIT searches in the first place. This trespass in violation of the fundamental jurisdictional limits of Rule 41 requires suppression under *Weiland*.

Finally, it is important to recognize that the FBI's intrusion included seizure of the defendants' MAC addresses, which are not typically shared with anyone. The MAC address is a critical piece of evidence, because it is used by the FBI to link the data that it has seized to a specific computer, while IP addresses may be shared by more than one computer and are "dynamic" (different IP addresses may be assigned to different

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

computers at different times). The Court did not address in its *Michaud* Order the prejudice that resulted from the seizure of data other than IP addresses.

2. The NIT searches infringed on a protected privacy interest and prejudiced the defendants regardless of the IP addresses.

The Court ultimately determined in *Michaud* that NIT defendants did not have a reasonable expectation of privacy in their IP addresses, and therefore they were not prejudiced by the violation of Rule 41 that allowed the FBI to seize those addresses. *Michaud* Order at *7. The defendants respectfully disagree with this latter conclusion for the following reasons.

The core privacy interests at issue in this case have nothing to do with whether IP addresses are semi-public, like unlisted phone numbers, or shared with third parties. Instead, the NIT searches violated protected privacy interests because they trespassed on constitutionally protected areas – the defendants' homes and the personal computers inside their homes. It makes no difference for Fourth Amendment purposes that the evidence seized during this trespass may have been obtainable elsewhere. And, as previously noted, Agent Alfin has conceded during testimony in other "Operation Pacifier" cases that, without the NIT, it would have been impossible for the FBI to obtain any IP addresses at all. Exh. K at 37, 57.

The Supreme Court's decisions in *United States v. Jones*, 132 S. Ct. 945 (2012), and *Riley v. California*, 134 S. Ct. 2473 (2014), strongly support our position. In *Jones*, the Government had attached a GPS tracking device to a car registered to the defendant while it was parked in a public parking lot. 132 S. Ct. at 948. The Court held that Jones had a privacy interest in the data collected by the GPS because the Government had "physically occupied private property for the purpose of obtaining information" when it placed the GPS device on Jones's car. *Id.* at 949.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

The Government had maintained that Jones had no reasonable expectation of privacy because the car was accessible and "visible to all" when it was parked in a lot and driving on public streets. *Id*. at 950. The Court, however, found that the Government had committed a "trespass" upon the "persons, houses, papers, and effects" protected by the Fourth Amendment when it attached the GPS and therefore had violated a protected privacy interest. *Id.*

The same is true here, when the Government attached malware to the defendants' computers, which were not only on private property at the time but were also cloaked in the traditional privacy protections afforded "papers and effects" located in a home. *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).

In addition, it made no difference in *Jones* that the location information collected by the Government was "voluntarily conveyed to the public" and shared with third parties. *Id.* at 951-52. The key fact for privacy purposes was that "the Government trespassorily inserted the information gathering device" into a private location. *Id*. at 952. An equivalent trespass occurred with the NIT, which is an "information gathering device" that was "trespassorily inserted" into the defendants' homes and computers.

This Court's conclusions about privacy are also at odds with the Supreme Court's conclusions in *Riley*. There, the Court held that the police must obtain a warrant to search personal cell phones, even if the phone is seized incident to a lawful arrest. The Court described cell phones as "minicomputers," and found that people had a reasonable expectation of privacy in the information stored on a phone. Most importantly for purposes of the instant cases, that privacy interest persists *regardless* of whether the information is also stored elsewhere or has been shared with third parties. 134 S. Ct. 2489.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

To illustrate this point, the Court noted that "[a]n Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns," and the phone could also reveal "[h]istoric location information." *Id*. at 2490. Both Internet search history and location data are routinely stored by cell phone service providers and by browser and search engine providers, separate and apart from data storage on the phone itself, but this fact made no difference to the Court's analysis.[5] *See also id.* at 2491 (acknowledging that the information was shared with third parties through the "cloud").

The *Riley* decision makes plain that a person has a privacy interest in his or her cell phone (or computer) data, regardless of whether that data was shared with third parties or could be acquired from other sources, whenever the data is in fact recovered from a private device. The dispositive consideration is whether the police intruded upon a constitutionally protected area at the time the seizure occurred. *See also id*. at 2494-95 (comparing the cell phone search at issue to the "reviled 'general warrants'" and noting that cell phones and computers are protected because "they hold for many Americans 'the privacies of life.'") (citation omitted); *see also Kyllo*, 533 U.S. at 44 (affirming suppression where warrant relied on energy consumption information obtained with a thermal imaging device that intruded upon the defendant's home, even though similar information was available from a third party utility company).

This law was not fully briefed in *Michaud.* The Court should now find that the NIT searches intruded upon a protected privacy interest and violated the Fourth Amendment.

3. Suppression is also Required on the Independent Ground that the Rule 41 Violation was Deliberate.

[5] This is how, for example, a search engine like Google can automatically complete search terms that one has previously entered, as soon as one starts typing them in again.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

The Ninth Circuit also requires suppression of evidence if officers acted in "intentional and deliberate disregard" of Rule 41, regardless of whether there is a showing of prejudice. *Weiland*, 420 F.3d at 1071 (citations omitted); *see also United States v. Martinez-Garcia*, 397 F.3d 1205, 1213 (9th Cir. 2005) (same). The Government deliberately violated Rule 41 when it obtained the NIT warrant. Although the Court decided otherwise in *Michaud*, the Court should revisit that conclusion in light of all the facts that have now emerged.

The Government's campaign to change Rule 41 started in 2013 and it was prompted by the decision in *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013) ("*In re Warrant*"). There, the court denied a Government application for an NIT warrant because it would violate Rule 41. In a detailed analysis of Rule 41 and its constitutional underpinnings, the *In re Warrant* decision put the Government on notice that using a warrant issued by a Magistrate Judge in one district to execute malware searches in another is not legal.

This decision was very much on DOJ's radar because it substantially curtailed the FBI's early hacking efforts. Implicitly acknowledging the soundness of the *In re Warrant* opinion (which the Government did not appeal), DOJ sent a letter in September, 2013, to the Advisory Committee on Criminal Rules, citing the case as a reason to change the Rule's jurisdictional limits. *See* exh. H (September 18, 2013 letter from Acting Asst. Attorney General Mythili Raman to the Hon. Reena Raggi, Chair, Advisory Committee on the Criminal Rules) at 2. This letter shows that DOJ fully understood, at least two years before it sought the NIT warrant here, that Rule 41 did not permit multi-district computer hacking. *See also id.* at 3 (where DOJ stated that the Rule should be changed to "remove an unnecessary *obstruction currently impairing* the

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

ability of law enforcement to investigate. . . multi-district Internet crimes") (emphasis added).

Moreover, DOJ's internal analysis of Rule 41 reached the same conclusion. According to DOJ's manual on Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (DOJ Electronic Evidence Manual), when "data is stored remotely in two or more different places within the United States and its territories, *agents should obtain additional warrants for each location where the data resides to ensure compliance with a strict reading of Rule 41(a).* For example, if the data is stored in two different districts, agents should obtain separate warrants from the two districts" (emphasis added). *Id*. at 84-85.[6]

The DOJ manual also addresses situations where, as here, "agents do not and even cannot know that data searched from one district is actually located outside the district[.]" *Id*. at 85. In these types of situations, the manual cautions agents that they will be inviting suppression if they deliberately disregard the Rule's jurisdictional limits. *Id.* Despite the manual's guidelines, a DOJ attorney reviewed and presumably approved the EDVA application. *See* exh. A at Bates 134 (cover sheet to application); *see also United States v. Coreas*, 419 F.3d 151, 151 (2d Cir. 2005) ("Child pornography is so repulsive a crime that those entrusted to root it out may, in their zeal, be tempted to bend or even break the rules. If they do so, however, they endanger the freedom of all of us.").

In light of *In re Warrant*, DOJ was on notice that a court agreed with the DOJ manual that a magistrate judge could not authorize a worldwide warrant under Rule 41. Nevertheless, DOJ has attempted to remove this "obstruction" to the FBI's hacking operations, without waiting for a rule change, by simply ignoring Rule 41 and taking its

[6] Available at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

chances on whether the courts would impose sanctions. Notably, a bipartisan bill is now pending in Congress in response to "Operation Pacifier" to block DOJ's proposed rule changes. *See* Dustin Volz, *Senators Introduce Bill to Block Expansion of FBI Hacking Authority*, Reuters News Service, May 19, 2016.[7]

Significantly, all courts that have reviewed "Operation Pacifier" cases have concluded that Rule 41 prohibited the NIT searches. *See, e.g.*, *Levin*, 2016 WL 2596010 at *13 (finding that "a veteran FBI agent with 19 years of federal law enforcement experience" should have known, given the plain language of the Federal Magistrate's Act and Fed. R. Crim. P. 41, that "it was not objectively reasonable for law enforcement" to believe that the warrant had been properly issued."); *United States v. Werdene*, at 2016 U.S. Dist. LEXIS 66311 * 15 (E.D. Pa. May 18, 2016) ("the courts generally agree that the magistrate judge in Virginia lacked authority under Rule 41 to issue the warrant," although they do not all agree that suppression is required).

Given these facts, the Court should now conclude that the Government deliberately violated Rule 41. Unlike some other circuits, suppression is the required remedy in this circuit for a deliberate rule violation, regardless of prejudice to the defendants. *See United States v. Martinez-Garcia*, 397 F.3d 1205, 1213 (9th Cir. 2005) (stating grounds for suppression, including deliberate rule violation and prejudice, in the disjunctive).

C. The NIT Search of Defendants' Washington Computers Was Not Authorized by the Warrant.

The conclusion that the FBI deliberately violated Rule 41 is further evidenced by the fact that agents presented Magistrate Judge Buchanan with a warrant and application that, on their face, limited NIT searches to the EDVA. The cover sheet of the NIT application states that the warrant is for "persons or property" that are "located

[7] Available at: http://www.reuters.com/article/us-usa-cyber-warrants-idUSKCN0YA23I

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

in the Eastern District of Virginia." 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 134. The Court should suppress for the simple reason that the FBI searched the locations outside the scope of the express language of the NIT warrant itself. *See United States v. Sedaghaty*, 728 F.3d 885, 913 (9th Cir. 2013) ("The affidavit as a whole cannot trump a limited warrant.").

The Court found in *Michaud* that the NIT warrant authorized worldwide searches because it refers to "activating computers" and this term, when read in conjunction with a single sentence that appears on page 29 of the warrant application, refers to computers that may be located anywhere. *See* exh. A at ¶ 46(a); *Michaud*, 2016 WL 337262 at *4. However, this construction contravenes the bright-line rule that courts are precluded from expanding the scope of a warrant by incorporating parts of the supporting application unless (a) the warrant expressly incorporates the application by reference, *and* (b) the application is physically attached to the warrant or accompanies it while agents execute the search. *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 699 (9th Cir. 2009). In other words, since the NIT warrant did not incorporate the application, courts are precluded from referring to it to define or expand the search location that is specified in the warrant itself.

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). The Court can only conclude that Magistrate Judge Buchanan knew the limits of her authority under

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

the Federal Magistrate's Act and Rule 41 when she issued the NIT warrant, and therefore identified the EDVA as the boundary for searching "any activating computers," a boundary that would be consistent with that authority.

To conclude otherwise is to find that Magistrate Judge Buchanan elected to issue a worldwide warrant without even pausing to change the geographical area written on the face of the warrant; add "… *and elsewhere*" to it (as was previously done with other NIT warrants);[8] or include a notation incorporating the warrant application. "Trial judges are presumed to know the law and to apply it in making their decisions." *Clark v. Arnold*, 769 F.3d 711, 727 (9th Cir. 2014), quoting *Walton v. Arizona*, 497 U.S. 639, 653 (1990), *overruled on other grounds by Ring v. Arizona*, 536 U.S. 584 (2002).

There is no reason to believe that the Magistrate Judge did not know what she was doing or, alternatively, that she intended to issue an unprecedented worldwide warrant without making that intention clear by amending the warrant or incorporating the application. While this Court may be correct that the worldwide powers *sought* by the FBI become apparent upon a very careful reading of the application, there is nothing within the four corners of the warrant or by permissible incorporation that allows a reviewing court to find that this sweeping authority was granted. Suppression is therefore required for all data that was seized outside of the Eastern District of Virginia.[9]

---

[8] *See* warrant and supporting application in *United States* v. *Cottom*, CR-13-108 (D. Neb. 2013) at ¶¶ 16-18. Copies of these records were submitted to the Court in *Michaud* (dkt. 32, exh. B) and are hereby incorporated by reference.

[9] *Bergquist v. County of Cochise*, 806 F.2d 1364 (9th Cir. 1986), *abrogated on other grounds, City of Canton, Ohio v. Harris*, 489 U.S.378 (1989), does not support the *Michaud* Order's conclusion that any reasonable interpretation of a warrant can save it. *Michaud*, 2016 WL 337262 at *4. *Bergquist* was a § 1983 civil action in which the Court of Appeals addressed the scope of qualified immunity for police officers and claims of negligent training and supervision. The case has nothing to do with the rules for construing the scope of a warrant for suppression purposes.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

The Government, of course, wants to have it both ways. On one hand, it will continue to urge this Court to construe the NIT warrant to allow searches of computers anywhere in the world, as it did in *Michaud*. At the same time, however, the Government wants to avoid the sanctions required for evading the jurisdictional limits of the Magistrate's Act and Rule 41. But no matter which way it turns, the Government must lose. If the warrant is indeed worldwide, then it was "void ab initio" under the Federal Magistrate's Act and also fundamentally violated Rule 41. If the warrant is limited, then the FBI was not allowed to search Washington computers pursuant to it.

Finally, the very purpose of the exclusionary rule supports suppression here. *See Herring v. United States*, 555 U.S. 135, 144 (2009) (the exclusionary rule serves to deter not only deliberate and reckless police conduct but also "in some circumstances recurring or systemic negligence."). The FBI presented an ostensibly worldwide warrant to a Magistrate Judge whose jurisdiction is circumscribed by statute, the federal rules, and the constitution. The FBI paid lip service to these restrictions by referencing the Eastern District of Virginia as the *only* particularly identified search location. Yet the Government persists in asking this Court to endorse its circumvention of the Magistrate's Act and Federal Rules (i.e. the law), an outcome that will only set the stage for further overreaching by the Government, as surveillance technology grows ever more sophisticated.

Accordingly, this case is a textbook example of where enforcing the exclusionary rule will have a beneficial effect on law enforcement practices. *See also United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1172 and 1177 (9th Cir. 2010) (warning the Government against "deliberate overreaching" when searching computers and requiring judges to exercise "greater vigilance" when reviewing computer warrant applications).

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

D. The NIT Warrant Was Not Supported by Probable Cause

1. Playpen did not "Unabashedly Announce" that it was a Child Pornography Site After the FBI Took Control of it.

We are mindful this Court found that this warrant was supported by probable cause in the *Michaud* case. However, in its findings and order, the Court did not address the leading case of *United States v. Gourde*, 440 F.3d 1065 (9th Cir. 2006) (en banc). Pursuant to *Gourde*, the Government did not have probable cause to search "any activating computer" that connected to the FBI's web site.

The NIT warrant application contains no particularized information about Playpen visitors and it does not include a collector profile. Instead, the application states that Playpen's "primary purpose is the advertisement and distribution of child pornography." Exh. A at ¶ 11. The application does not claim that Playpen advertised itself as that term is commonly understood, such as by posting ads on other sites or distributing "pop up" ads. Instead, the application maintains that Playpen advertised itself as a child pornography site because of what appeared on the site itself, and, more specifically, what appeared on the site's home (or "log in") page. *See id*. at ¶ 12. Since the warrant authorized NIT searches whenever unknown visitors accessed the home page, probable caused depends on what visitors would have seen on that page at the time the searches were executed.

The home page contains no references to child pornography, sexually explicit content, or anything of a similar nature. *See* exh. G. Instead, the only fact showing that the site advertised child pornography is the description of two pictures that had *previously* appeared on the site's banner, "depicting partially clothed prepubescent females with their legs spread apart." Exh. B at ¶ 12. The rest of the facts about the site consist of general (and frequently erroneous) information about the Tor network; a recitation of commonplace technical text on the home page; and what was inside the

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

site. The application's descriptions of the site's contents add little or nothing to probable cause in this case because the FBI obtained authorization to execute NIT searches before visitors could see the contents. *Compare Gourde*, 440 F.3d at 1070 (affidavit established that the defendant had bought a membership *after* viewing the pornography on the site).

The law in this circuit is clear that when a search is based on merely visiting a website, there is probable cause for the search only if the illegal nature of that site would be obvious to even unwitting visitors. In *Gourde*, the Ninth Circuit considered whether there was probable cause to search the computer of someone based on his membership in a site that distributed child pornography. The question of probable cause turned on how the site appeared to visitors, and what Gourde had done apart from merely visiting the site that manifested an intent to possess child pornography.

Unlike here, the site in *Gourde* was very explicit about what it offered. First, the name of the site was "Lolitagurls.com," and the term "Lolita" is closely 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.'").

In addition, unlike Playpen's home page, the Lolitagurls.com home page brazenly advertised 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,

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

in stark contrast to Playpen, the site in *Gourde* "unabashedly announced that its essential purpose was to trade child pornography."[10]

Here, Playpen's illegal purpose was not at all clear once the pictures of child pornography were removed from its home page, and it in no way "unabashedly announced" that it was an illegal site. *See* exh. G.

In the *Michaud* Order, the Court concluded that the name "Playpen" itself was suggestive of child pornography. 2016 WL 337262 at *3. However, there are no facts in the record to support this conclusion. The NIT warrant application makes no claim that the term "Playpen" is associated with child pornography. And, to the contrary, "Playpen" is widely associated with mainstream "adult entertainment." The name "Playpen" is used by a "men's lifestyle" magazine that is a knock-off of "Playboy" (*see* exh. I); 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 websites (such as "Angel's Playpen" and "Xtreme Playpen") that feature far more explicit (and entirely legal) pictures of young women than appear on the home page at issue here. *Compare* exhs. G *and* I.

The prevalence with which the term "Playpen" is used in connection with mainstream sexual content suggests, if anything, that most visitors to the FBI's version of the site likely did not know what they were getting into. This conclusion is further supported by the relatively small number of visitors who have been prosecuted since the FBI closed its site in March, 2015. Although almost 18 months have passed since then, only 186 Playpen visitors out of a 100,000 have been charged. *See Lorente,* dkt. 84 (Govt. summary of Operation Pacifier cases charged to date). The obvious question is

[10] This description of the website is from *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[.]"

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

what happened to the remaining 99,814 visitors, if Playpen was so obviously dedicated to child pornography that anyone accessing it was likely to be committing a crime?

The Ninth Circuit also deemed it significant that the site in *Gourde* charged a membership fee and visitors saw "images of nude and partially-dressed girls, some prepubescent" *before* they joined the site. 440 F.3d at 1067. The court found that Gourde had demonstrated his intent to view and download child pornography because, after having viewed samples of the site's pictures, he took the "affirmative steps" of entering credit card information, paying a monthly fee, and maintaining his membership. Hence, "[t]he 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." *Id*. at 1071. The affidavit also demonstrated that Gourde 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.

Here the opposite is true. The FBI offered free and immediate access to Playpen, and it did not offer previews of the site's contents before executing the NIT searches. Since Playpen did not charge fees or previews, and there was no child pornography posted on its home page by the time the NIT warrant was issued, it is highly likely that most of the people who visited the site with its altered home page were not seeking to download or distribute illegal pornography, "balked" at having anything further to do with the site, and by then had already had their computers searched by the NIT.

In sum, the probable cause boundaries established in *Gourde* make sense and the Court should enforce them. The Internet is awash with websites that cater to every imaginable fetish, much of which is repugnant but nonetheless legal and even constitutionally protected. As the Second Circuit recently explained, "Although it is

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

increasingly challenging to identify that line [between fantasy and criminal 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). "We 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).

This Court should be equally loath to approve the sweeping search and seizure powers that the Government exercised in this case; it should instead conclude that the NIT warrant violated the Fourth Amendment by authorizing overbroad and generalized searches of Playpen visitors.

2. The NIT Warrant's Triggering Condition Failed.

The warrant's lack of probable cause to search 100,000 or more computers is compounded by the fact that (as the Government has previously conceded) it is an anticipatory warrant. 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 logging in *when the site appeared as described in the warrant application*. *See, e.g.*, exh. B at Bates 169 (an "activating computer" is one that belongs to anyone who logs into Playpen). 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 Playpen visitors if the site continued (as in *Gourde*) to "unabashedly announce" that it was dedicated to

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

child pornography. Assuming that probable cause was established by the warrant application's description of child pornography that was previously posted on the home page, the facts related to the triggering act of accessing the site changed materially once those pictures were removed. By the time the NIT searches were executed, there was nothing on the home page that would lead an unwitting visitor to recognize Playpen as anything more than another fetish site (many of which specialize in hardcore, but legal, "teen" (18 or older) pictures).

In fact, the single picture of a fully clothed young woman or teenager that the FBI maintained on the home page is far less suggestive than many images that pervade mainstream media. *Compare* exh. G *with* exh. J (a sampling of pictures that appear with a Google search of "child models"); *see also 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").

Given these facts, the triggering event established in the warrant application (entering the site while child pornography is clearly displayed on the home page) could not, and did not, occur. And, since the triggering event could not occur, any searches based on the NIT warrant exceeded the scope of its authorization. It is immaterial whether this failure was the result of intentional omissions on the part of the FBI or mere carelessness. Here again, the warrant was "void." *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 Court Should Hold a *Franks* Hearing Because the NIT Affidavit Contains, at a Minimum, Recklessly Misleading Statements and Omissions.

Although the Court declined to hold a *Franks* hearing in *Michaud*, facts that have emerged since then further demonstrate the need for one. Indeed, it will be

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

impossible to get to the bottom of how the Government handled this unprecedented investigation without a *Franks* hearing.

First, during recent testimony in other NIT cases, the lead FBI agent for Operation Pacifier, Daniel Alfin, has testified that he was aware that Playpen's home page had changed and no longer displayed child pornography before the NIT warrant was issued.[11]

Second, Agent Alfin has also recently testified that the FBI had to "reboot" the site after it was moved to a government server, prior to the NIT warrant application. Exh. K at 58. At that point, the FBI was the exclusive owner and operator of the site and all of the agents and technicians who got the site back up and running would have inevitably reviewed the appearance and content of the home page.

Third, Agent Alfin has recently stated, during testimony in the Western District of Arkansas, that he was actively involved in the preparation of the NIT warrant application. In fact, he testified that he provided "the bulk of the information that went into the warrant." Exh. K at 81.

---

[11] During the June 23 hearing in *U.S. v. Jean*, Agent Alfin confirmed that he saw the changes to the home page the day before he helped prepare the NIT warrant application. He also acknowledged that "importantly, on this page, the logo has been changed and so this is the logo that was active on the website when I encountered the [original] administrator's laptop in his residence on February 19th, 2015." Exh. K at 34.

The *Michaud* Order, relying on earlier testimony by Alfin, states that he "saw the newer version of [Playpen's] main page but did not notice the picture changes." *Michaud*, WL 337263 at *3. In fact, Alfin had testified that he was aware of the change. Exh. F (*Michaud*, January 22, 2016 Hearing Transcript) at 87-92. Alfin did seek to minimize his knowledge by claiming that "it did not jump out to me as a significant change to the web site," *id.* at 92. But this assertion is not credible given his claims elsewhere about his extensive experience and expertise when it comes to Internet investigations. It is also contradicted, as noted above, by more recent testimony.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

From a legal standpoint, it is largely immaterial whether Alfin was directly involved in preparing the warrant application or if he understood the significance of the home pages changes. Since he was the lead agent for Operation Pacifier, any knowledge he acquired in that capacity is attributed to all other agents that were working on the operation. *See generally United States v. Ramirez*, 473 F.3d 1026, 1032 (9th Cir. 2007) (discussing the "collective knowledge doctrine"). Nevertheless, these recent admissions further demonstrate the need for a *Franks* hearing.

In short, the evidence shows that the FBI knew or should have known that Playpen's home page no longer displayed child pornography and failed to disclose this fact to Magistrate Judge Buchanan. The description of the site's home page was the key component of the affiant's allegations in support of probable cause to search 100,000 computers.

A *Franks* hearing is appropriate whenever the defense has made a preliminary showing that the FBI deliberately or recklessly included false information in a warrant application. Indeed, all the defense need show is that agents "recklessly failed to verify" material information in order to warrant a *Franks* hearing. *United States v. Meling*, 47 F.3d 1546, 1553 (9th Cir. 1995). The facts establish that, at a minimum, the FBI recklessly failed to verify the contents of Playpen's home page before submitting the NIT application. The Court should therefore order a *Franks* hearing.

IV. CONCLUSION

For the reasons stated above, the Court should grant the defendants' motions for a *Franks* hearing and for suppression.

DATED this 22nd day of August, 2016.

Respectfully submitted,

s/ *Colin Fieman*
Attorney for David Tippens

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

s/ *Robert Goldsmith*
Attorney for Gerald Lesan

s/ *Mohammad Hamoudi*
Attorney for Bruce Lorente

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

CERTIFICATE OF SERVICE

I hereby certify that on August 22, 2016, I electronically filed the foregoing 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, Paralegal*
Federal Public Defender Office

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. DAVID TIPPENS, Defendant.	No. CR16-5110RJB **[PROPOSED ORDER] GRANTING MOTION TO SUPPRESS EVIDENCE**
UNITED STATES OF AMERICA, Plaintiff, v. GERALD LESAN, Defendant.	No. CR15-387RJB **[PROPOSED ORDER] GRANTING MOTION TO SUPPRESS EVIDENCE**
UNITED STATES OF AMERICA, Plaintiff, v. BRUCE LORENTE, Defendant.	No. CR15-274RJB **[PROPOSED ORDER] GRANTING MOTION TO SUPPRESS EVIDENCE**

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

The defendants' having brought a Motion to Suppress Evidence, and the Court having considered the arguments, memoranda, and evidence presented both in support of and in opposition to the motion, now, therefore,

ORDERS that all fruits of the Government's "Network Investigative Technique" searches, including any allegedly inculpatory statements made by the defendants following the searches, are SUPPRESSED. Law enforcement's actions violated the defendant's rights under the Fourth Amendment to the United States Constitution and may not be used by the government in its case in chief against the defendant.

DONE this _____ day of September, 2016.

_____
JUDGE ROBERT J. BRYAN
UNITED STATES DISTRICT JUDGE

Presented by:

s/ *Colin Fieman*
Colin Fieman
Attorney for David Tippens

s/ Robert Goldsmith
Robert Goldsmith
Attorney for Gerald Lesan

s/ Mohammad Hamoudi
Mohammad Hamoudi
Attorney for Bruce Lorente

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710