The Honorable Marsha J. Pechman

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. B.L., Defendant.	NO. CR15- GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

The United States of America, by and through Annette L. Hayes, United States Attorney for the Western District of Washington, Matthew P. Hampton and Andre Penalver, Assistant United States Attorneys for said District, and Keith A. Becker, Trial Attorney, hereby files this Response to the Defendant's Motion to Suppress Evidence. For the reasons stated herein, the Defendant's motion should be denied.

I. INTRODUCTION

After a months-long investigation, the FBI briefly assumed administrative control of Playpen, a website dedicated to the sharing of child pornography. The FBI also sought and obtained a warrant permitting it to deploy a "Network Investigative Technique" (the "NIT") that would cause a computer logging into Playpen to reveal certain identifying information—most importantly, its concealed IP address. Among the IP addresses identified accessing Playpen was one belonging to B.L.. Following the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

execution of a search warrant at his Seattle home, L. was arrested and indicted on charges of receipt and possession of child pornography. For the reasons that follow, his motion to suppress, Dkt. 33, should be denied.

First, the affidavit supporting the NIT warrant application established the need for the NIT to identify Playpen users and set forth ample probable cause to conclude that any users Playpen knew of its illicit content and intended to access that content. As the affidavit explained, Playpen was no ordinary website but a hidden site operating on an anonymous network that was dedicated to the sharing of child pornography. The magistrate judge reasonably concluded that there was a fair probability that anyone who logged into Playpen did so with knowledge of its content and intent to view that content.

Second, L. makes no showing—much less a substantial, preliminary one—to justify a *Franks* hearing. He points to a change to the Playpen logo that occurred hours before the NIT warrant was authorized that was not included in the affidavit. But he does not offer any proof that this omission was intentional or reckless, nor can he. It was, at most, and innocent oversight. As important, the change—the replacement of two sexually suggestive photos of a prepubescent girl with a single sexually suggestive photo of a prepubescent girl—was immaterial. So even if L. could somehow show the affiant acted intentionally or recklessly, he would not be entitled to relief. His remaining *Franks* arguments consist of little more than a disagreement with the opinions and conclusions of the veteran FBI agent contained within his affidavit, none of which suffice to justify a *Franks* hearing.

Third, the NIT warrant described the places to be searched and the items to be seized with particularly and was supported by probable cause. The Fourth Amendment demands nothing more. The Court should not embrace Lorente's novel and unsupported constitutional rule—cloaked as a challenge to the warrant's particularity and overbreadth—that would find an otherwise valid warrant defective simply because it would authorize the search of a potentially large number of locations.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

Fourth, the NIT warrant complied with Rule 41. As the Supreme Court and the Ninth Circuit have explained, Rule 41 should be construed broadly so as to uphold otherwise constitutionally valid search warrants where possible. And even if there were a technical violation of its jurisdictional provisions, suppression is entirely unwarranted on the facts of this case.

Fifth, the warrant plainly authorized deployment of the NIT to his computer even though its physical location was outside the Eastern District of Virginia. No sensible reading of the NIT warrant permits the crabbed and self-serving interpretation he advances.

Finally, Lorente's remaining criticisms of the NIT warrant are similarly unavailing and do nothing to aid his cause. And even if the warrant were somehow flawed, *Leon*'s good faith exception is an independent bar to suppression. The NIT warrant affidavit set forth probable cause for its request to search particular locations for particular information. And a neutral and detached magistrate relied on that affidavit in authorizing that warrant. Law enforcement's reliance on that authorization was therefore objectively reasonable, and suppression is thus unwarranted.

For these and the other reasons outlined below, Lorente's motion should be denied.

II. BACKGROUND

The charges in this case arise from an investigation into Playpen, a global online forum through which registered users (including L.) advertised, distributed, and/or accessed illegal child pornography. The scale of child sexual exploitation on the site was massive: more than 150,000 total members created and viewed tens of thousands of postings related to child pornography. Images and videos shared through the site were highly categorized according to victim age and gender, as well as the type of sexual activity. The site also included forums for discussion for all things related to child sexual exploitation, including tips for grooming victims and avoiding detection.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

A. Playpen users, including L., used the Tor network to access child pornography while avoiding law enforcement detection.

Playpen operated on the anonymous Tor network. Tor was created by the U.S. Naval Research Laboratory as a means of protecting government communications. It is now available to the public. The Tor network—and the anonymity it provides—is a powerful tool for those who wish to share ideas and information, particularly those living in places where freedom of speech is not accorded the legal protection it is here. But this anonymity has a downside. The Tor network is a haven for criminal activity in general, and the online sexual exploitation of children in particular. *See Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds*, WIRED MAGAZINE, December 30, 2014, available at: http://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/ (last visited November 13, 2015).

Use of the Tor network masks the user's actual Internet Protocol ("IP") address, which could otherwise be used to identify a user, by bouncing user communications around a network of relay computers (called "nodes") run by volunteers.[1] To access the Tor network, users must install Tor software either by downloading an add-on to their web browser or the free "Tor browser bundle." Users can also access Tor through "gateways" on the open Internet that do not provide users with the full anonymizing benefits of Tor. When a Tor user visits a website, the IP address visible to that site is that of a Tor "exit node," not the user's actual IP address, Tor is designed to prevent tracing the user's actual IP address back through that Tor exit node. Accordingly, traditional IP-address-based identification techniques used by law enforcement on the open Internet are not viable.

Within the Tor network itself, certain websites, including Playpen, operate as "hidden services." Like other websites, they are hosted on computer servers that communicate through IP addresses. They operate the same as other public websites with one critical exception: namely, the IP address for the web server is hidden and replaced

[1] Additional information about Tor and how it works can be found at www.torproject.org.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

with a Tor-based web address, which is a series of sixteen algorithm-generated characters followed by the suffix ".onion." A user can only reach a "hidden service" by using the Tor client and operating in the Tor network. And unlike an open Internet website, it is not possible to use public lookups to determine the IP address of a computer hosting a "hidden service."

A "hidden service" like Playpen is also more difficult for users to find. Even after connecting to the Tor network, users must know the exact web address of a "hidden service" in order to access it. Accordingly, in order to find Playpen, a user had to first get the web address for it from another source—such as another Playpen user or online postings identifying Playpen's content and location. Accessing Playpen thus required numerous affirmative steps by the user, making it extremely unlikely that any user could have simply stumbled upon it without first understanding its child pornography-related content and purpose.

Although the FBI was able to view and document the substantial illicit activity occurring on Playpen, investigators faced a tremendous challenge when it came to identifying Playpen users. Because Tor conceals IP addresses, normal law enforcement tools for identifying Internet users would not work. So even if law enforcement managed to locate Playpen and its IP logs, traditional methods of identifying its users would have gone nowhere.

Acting on a tip from a foreign law enforcement agency as well as information from its own investigation, the FBI determined that the computer server that hosted Playpen was located at a web-hosting facility in North Carolina. In February 2015, FBI agents apprehended the administrator of Playpen and seized the website from its web-hosting facility. Rather than immediately shut the site down, which would have allowed the users of Playpen to go unidentified (and un-apprehended), the FBI allowed it to continue to operate at a government facility in the Eastern District of Virginia for the brief period from February 20, 2015, and March 4, 2015.

In addition, the FBI obtained court authorizations from the United States District Court for the Eastern District of Virginia to (1) monitor site users' communications and (2) deploy a Network Investigative Technique ("NIT") on the site, in order to attempt to identify registered site users who were anonymously engaging in sexual abuse and exploitation of children, and to locate and rescue children from the imminent harm of ongoing abuse and exploitation.[2] Inexplicably, L. asserts that the FBI's seizure and takeover of Playpen "was not disclosed to the judge who issued the NIT warrant." Dkt. 33, p. 4. That is untrue. The NIT warrant affidavit explicitly stated that the FBI would be taking over Playpen and operating it from a server in the Eastern District of Virginia during the period of authorization. Ex. 1, p. 23, ¶ 30.

Using the NIT, the FBI identified an IP address associated with Playpen user "Jimbox" and traced it to B.L.. FBI Special Agent Caryn Highley obtained a residential search warrant for Lorente's home from Magistrate Judge Mary Alice Theiler. *In the matter of the search of 1641 Bellevue Ave, Apt 312, Seattle, WA 98122*, MJ15- 335MAT. FBI executed the warrant at Lorente's home, and after being advised of his constitutional rights, L., the only occupant of the home, agreed to be interviewed. Among other things, he admitted that he had viewed and downloaded thousands of images of child pornography and stated his most recent download was just two days before the warrant. He also admitted that he had used Tor to access and download images. The initial forensic preview confirmed the presence of images of child pornography on devices seized from L., and he was taken into custody. L. was later indicted on one count each of possession and receipt of child pornography. *See* Dkt. 1.

[2] Publicly filed copies of the NIT search warrant, application, affidavit and return (No. 15-SW-89) are attached as Exhibit 1. A publicly filed copy of the separate Title III application, affidavit, and order are attached as Exhibit 2.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

B. The nature of Playpen and the Tor network required law enforcement to seek court approval to deploy a NIT to identify criminals engaged in the creation, advertisement, and distribution of child pornography.

The 31-page NIT search warrant affidavit was sworn to by a veteran FBI agent with 19 years of federal law enforcement experience and particular training and experience investigating child pornography and the sexual exploitation of children. Ex. 1, p. 1, ¶ 1. It clearly and comprehensively articulated probable cause to deploy the NIT to obtain IP address and other computer-related information that would assist in identifying registered site users using anonymizing technology to conceal online child sexual exploitation on a massive scale.

1. The NIT warrant set forth in great detail the technical aspects of the investigation that justified law enforcement's request to use the NIT.

In recognition of the technical and legal complexity of the investigation, the affidavit included: a three-page explanation of the offenses under investigation, Ex. 1, pp. 2-4, ¶ 4; a seven-page section setting out definitions of technical terms used in the affidavit, *id.*, pp. 4-10, ¶ 5; and a three-page explanation of the Tor network, how it works, and how users could find a hidden service such as Playpen, *id.*, pp. 10-13, ¶¶ 7-10. The affidavit spelled out the numerous affirmative steps a user would have to go through just to find the site. Indeed, the agent explained,

> Even after connecting to the Tor network, however, a user must know the web address of the website in order to access the site. Moreover, Tor hidden services are not indexed like websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user may not simply perform a Google search for the name of one of the websites on Tor to obtain and click on a link to the site. A user might obtain the web address directly from communicating with other users of the board, or from Internet postings describing the sort of content available on the website as well as the website's location. For example, there is a Tor "hidden service" page that is dedicated to pedophilia and child pornography. That "hidden service" contains a section with links to Tor hidden services that contain child pornography. [Playpen] is listed in that section.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

Id., pp. 12-13, ¶ 10. Thus, the agent continued, "[a]ccessing [Playpen] . . . requires numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble upon [it] without understanding its purpose and content." *Id.*

2. Playpen was dedicated to the advertisement and distribution of child pornography, a fact that would have been apparent to anyone who viewed the site.

The affidavit also described, in great detail and in stark terms the purpose of Playpen and why its users were appropriate targets for the NIT. Playpen was "dedicated to the advertisement and distribution of child pornography," "discussion of . . . methods and tactics offenders use to abuse children," and "methods and tactics offenders use to avoid law enforcement detection while perpetrating online child sexual exploitation crimes." *Id.*, p. 6, ¶ 10. More to the point, "administrators and users of [Playpen] regularly sen[t] and receive[d] illegal child pornography via the website." *Id.* The agent also explained the sheer scale of the illicit activity occurring on Playpen: site statistics as of February 3, 2015, for Playpen—which was believed to have been in existence only since August of 2014—showed that it contained 158,094 members, 9,333 message threads, and 95,148 posted messages.[3] *Id.*, p. 13, ¶ 11.

Playpen's illicit purpose was also apparent to anyone who visited it during the six months it operated before the FBI seized control of it. "[O]n the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent females with their legs spread apart." *Id.*, p. 13, ¶ 12. And the following text appeared beneath those young girls: "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." While those terms may have seemed insignificant to the untrained eye, the affiant explained, based on his training and his

[3] As the affidavit explained, a bulletin board website such as Playpen is a website that provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Ex. 1, p. 4, ¶ 5(a).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

experience, that the phrase "no cross-board reposts" referred to a "prohibition against material that is posted on other websites from being 're-posted'" to Playpen and that ".7z" referred to a "preferred method of compressing large files or sets of files for distribution." *Id.*, pp. 13-14, ¶ 12. The combination of sexualized images of young girls along with these terms of art referencing image posting and large file compression unmistakably marked Playpen as just what it was—a hub for the trafficking of illicit child pornography.

The affidavit also explained that users were required to register an account by creating a username and password before they could access the site and highlighted the emphasis the registration terms placed on users avowing being identified. Users clicking on the "register an account" hyperlink on the main page were required to accept registration terms, the entire text of which was included in the affidavit. *Id.*, pp. 14-15, ¶¶ 12-13. Playpen repeatedly warned prospective users to be vigilant about their security and the potential of being identified, explicitly stating, "the forum operators do NOT want you to enter a real [e-mail] address," users "should not post information [in their profile] that can be used to identify you," "it is impossible for the staff or the owners of this forum to confirm the true identity of users," "[t]his website is not able to see your IP," and "[f]or your own security when browsing or Tor we also recomend [sic] that you turn off javascript and disable sending of the 'referer' header." *Id.*, pp. 14-15, ¶ 13. This focus on anonymity is entirely consistent with the desire on the part of Playpen administrators and users to evade detection of their illicit activities.

Once a user accepted those terms and conditions, a user was required to enter a username, password, and e-mail address. *Id.*, p. 15, ¶ 14. Upon successful registration, all of the sections, forums, and sub-forums, along with the corresponding number of topics and posts in each, were observable. *Id.*, p. 15, ¶ 14. The screenshot of Playpen's main board index, attached as an exhibit to Lorente's motion, is telling. *See* Dkt 35, Ex. D. The vast majority of those sections and forums were categorized repositories for sexually explicit images of children, sub-divided by gender and the age of the victims.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

For instance, within the site's "Chan" forum were individual sub-forums for "jailbait" or "preteen" images of boys and girls. Ex. 1, p. 15, ¶ 14. There were separate forums for "jailbait videos" and "Jailbait photos" featuring boys and girls. *Id.* The "Pre-teen Videos" and "Pre-teen Photos" forums were each divided into four sub-forums by gender and content, with "hardcore" and "softcore" images/videos separately categorized for Boys and Girls. *Id.*, p. 16, ¶ 14. A "Webcams" forum was divided into Girls and Boys sub-forums. *Id.* The "Potpurri" forum contained subforums for incest and "Toddlers." *Id.*

The affidavit also described, in graphic detail, particular child pornography that was available to all registered users of Playpen, including images of prepubescent children and even toddlers, being sexually abused by adults. *Id.*, pp. 17-18, ¶ 18. Although the affidavit clearly stated that "the entirety of [Playpen was] dedicated to child pornography," it also specified a litany of site sub-forums which contained "the most egregious examples of child pornography" as well as "retellings of real world hands on sexual abuse of children." *Id.* pp. 20-21, ¶ 27.

The affidavit further explained that Playpen contained a private messaging feature that allowed users to send messages directly to one another. The affidavit specified that "numerous" site posts referenced private messages related to child pornography and exploitation, including an example where one user wrote to another, "I can help if you are a teen boy and want to fuck your little sister, write me a private message." *Id.*, pp. 18-19, ¶ 21. According to the affiant's training and experience and law enforcement's review of the site, the affiant stated his belief that the site's private message function was being used to "communicate regarding the dissemination of child pornography." *Id.*, p. 19, ¶ 22. The affidavit also noted that Playpen included multiple other features intended to facilitate the sharing of child pornography, including an image host, a file host, and a chat service. *Id.*, pp. 19-20, ¶¶ 23-25. All of those features allowed site users to upload, disseminate, and access child pornography. And the affidavit included detailed examples

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

and graphic descriptions of prepubescent child pornography disseminated by site users through each one of those features. *Id.*

3. The affidavit and attachments explained what the NIT would do and precisely identified the seven pieces of information it would collect and send back to government-controlled computers.

The affidavit contained a detailed and specific explanation of the NIT, its necessity, how and where it would be deployed, what information it would collect, and why that information constituted evidence of a crime.

Specifically, the affidavit noted that without the use of the NIT "the identities of the administrators and users of [Playpen] would remain unknown" because any IP address logs of user activity on Playpen would consist only of Tor "exit nodes," which "cannot be used to locate and identify the administrators and users." Ex. 1, p. 22, ¶ 29. Further, because of the "unique nature of the Tor network and the method by which the network . . . route[s] communications through multiple other computers, . . . other investigative procedures that are usually employed in criminal investigations of this type have been tried and have failed or reasonably appear to be unlikely to succeed." The affiant thus concluded, "using a NIT may help FBI agents locate the administrators and users" of Playpen. *Id.*, pp. 23-24, ¶¶ 31-32. Indeed, he explained, based upon his training and experience and that of other officers and forensic professionals, the NIT was a "presently available investigative technique with a reasonable likelihood of securing the evidence necessary to prove . . . the actual location and identity" of Playpen users who were "engaging in the federal offenses enumerated" in the warrant. *Id.*, p. 23, ¶ 31.

In terms of the deployment of the NIT, the affidavit explained that the NIT consisted of additional computer instructions that would be downloaded to a user's computer along with the other content of Playpen that would be downloaded through normal operation of the site. Ex. 1, p. 24, ¶ 33. Those instructions, which would be downloaded from the website located in the Eastern District of Virginia, would then cause a user's computer to transmit specified information to a government-controlled

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

computer. *Id.* The discrete pieces of information to be collected were detailed in the warrant and accompanying Attachment A, along with technical explanations of the terms. They were limited to the following: (1) the actual IP address assigned to the user's computer; (2) a unique identifier to distinguish the data from that collected from other computers; (3) the operating system running on the computer; (4) information about whether the NIT had already been delivered to the computer; (5) the computer's Host Name; (6) the computer's active operating system username; and (7) the computer's Media Access Control (MAC) address. *Id.*, pp. 24-25, ¶ 34.

The affidavit explained exactly why the information "may constitute evidence of the crimes under investigation, including information that may help to identify them . . . computer and its user." *Id.*, p. 26, ¶ 35. For instance:

> the actual IP address of a computer that accesses [Playpen] can be associated with an ISP and a particular ISP customer. The unique identifier and information about whether the NIT has already been delivered to an "activating" computer will distinguish the data from that of other "activating" computers. The type of operating system running on the computer, the computer's Host Name, active operating system username, and the computer's MAC address can help to distinguish the user's computer from other computers located at a user's premises.

Id.

The affidavit specifically requested authority to deploy the NIT each time any user logged into Playpen with a username and a password. *Id.*, p. 26, ¶ 36. However, the affidavit disclosed to the magistrate that, "in order to ensure technical feasibility and avoid detection of the technique by suspects under investigation," the FBI might "deploy the NIT more discretely against particular users, including those who "attained a higher status" on the site or "in particular areas of [Playpen]" such as the sub-forums with the most egregious activity which were described elsewhere in the affidavit. *Id.*, pp 24-25, ¶ 32, n. 8. Finally, the affidavit requested authority for the NIT to "cause an activating computer – wherever located – to send to a computer controlled by or known to the government . . . messages containing information that may assist in identifying the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

computer, its location, other information about the computer and the user of the computer." *Id.*, pp. 29-30, ¶ 46(a).

C. Hours before the NIT warrant was signed, Playpen's administrator changed the site logo, replacing two sexually suggestive images of a prepubescent girl with one sexually suggestive image of a prepubescent girl.

As noted above, among the things described in the NIT warrant affidavit was Playpen's site logo: "on the main page of the site, located to either side of the site name, were two images depicting partially clothed prepubescent females with their legs spread apart." Ex. 1, p. 13, ¶ 12. A screenshot showing this logo as of February 3, 2015, is attached as Exhibit 3. Between September 16 and February 3, 2015, FBI agents reviewed Playpen in an undercover capacity to document the activity on the site. Ex. 1, p. 13, ¶ 11. Sometime before February 18, 2015, Playpen's administrator changed the URL—the site address. Noticing that the URL had changed, the affiant visited Playpen on February 18, 2015, and confirmed that the content had not changed. Ex. 1, p. 13, ¶ 11 n.3. This includes the site logo.

In the evening of February 19, 2015, the FBI executed a search at the Florida home of the Playpen administrator and apprehended him. *Id.*, p. 23, ¶ 30. At that point, the FBI also assumed control of Playpen. Postings by the administrator from earlier in the day show that just before he was arrested, the administrator changed Playpen's site logo, replacing the images described above with a single image showing a prepubescent girl, wearing a short dress and black stockings, reclined on a chair with her legs crossed and posed in a sexually suggestive manner. A screenshot of this altered logo is attached as Exhibit 4. The text described in the affidavit as part of the logo, "[n]o cross-board reposts, .7z preferred, encrypt filenames, include preview," which the affidavit explained pertain to image distribution, remained unchanged. *Compare* Ex. 1, p. 13, ¶ 12 *and* Ex. 3 *with* Ex. 4.

The NIT warrant was sworn to and authorized at 11:45 a.m. on February 20, 2015, the day after the logo change. The affidavit did not reference this change.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

III. ARGUMENT

A veteran FBI agent with nearly two decades of experience explained to a neutral and detached magistrate why there was probable cause to believe that registered users of Playpen 1) knew Playpen was a website dedicated to the sexual exploitation of children and 2) intended to use Playpen for its express purposes—viewing and sharing child pornography. He supported this conclusion with a detailed description of the steps required to find Playpen and register as a user and the numerous indicators of Playpen's illicit purpose. That purpose was obvious to even a casual observer, but the agent also was able to bring to bear his considerable training and experience and determine that the likelihood that any user of Playpen was ignorant of the fact that it was a forum dedicated to child pornography was exceedingly low.

Relying on this information, the magistrate authorized the FBI to deploy a NIT to gather a limited set of identifying information from any user who logged into Playpen while it operated under FBI control. There in the warrant, plain as day, was a clear description of which computers would be searched—any computers that logged into Playpen—and the seven pieces of information that would be seized. The Fourth Amendment asks no more.

As detailed below, nothing in Lorente's motion undermines this conclusion. The defects he identifies, if indeed they are defects, are of neither constitutional magnitude nor the result of an intention on the part of the FBI to mislead the magistrate or skirt the rules. His contrary assertions find no support in the record. Defendants seeking the extraordinary remedy of suppression must clear a high hurdle. L. falls far short, and his motion should denied.

A. The NIT warrant affidavit amply supports the magistrate's finding of probable cause for issuance of the NIT warrant.

Probable cause exists when "the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found." *Ornelas v. United States*, 517 U.S. 690, 696 (1996). It is a fluid concept

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

that focuses on "the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." *Illinois v. Gates*, 462 U.S. 213, 231 (1983) (internal quotation marks omitted).

Importantly, probable cause does not require a showing of "certainty or even a preponderance of the evidence." *United States v. Gourde*, 400 F.3d 1065, 1069 (9th Cir. 2006) (*en banc*). It demands only a "'fair probability' that contraband or evidence is located in a particular place," a finding that, in turn, depends on "the totality of the circumstances, including reasonable inferences and is a 'common sense, practical question.'" *Kelley*, 482 F.3d at 1050 (quoting *Gourde*, 440 F.3d at 1069). Recognizing that reasonable minds may differ regarding whether a particular affidavit establishes probable cause, the Supreme Court "concluded that the preference for warrants is most appropriately effectuated by according 'great deference' to a magistrate's determination." *United States v. Leon*, 468 U.S. 897, 914 (1984); *see also Gourde*, 440 F.3d at 1069.

1. The facts contained in the affidavit, along with reasonable inferences to be drawn therefrom, support probable cause to believe that registered users of Playpen intended to view and trade child pornography.

The NIT warrant affidavit amply supported a finding of probable cause. The affiant, a 19-year FBI veteran with specialized training and experience in the field, set forth in detail why there was probable cause to believe anyone who logged into Playpen did so intending to view and/or trade child pornography. Accordingly, his 31-page affidavit provided ample justification for deploying a NIT that would obtain seven discrete pieces of information and assist law enforcement in identifying those engaged on the sexual exploitation of children. [4]

Here, the affiant's assessment (and the magistrate's reasonable reliance upon it) was supported by specific, articulable facts and inferences drawn from his training and

[4] Amicus Curiae Electronic Frontier Foundation ("EFF") points out, at length, the unremarkable proposition that use of the NIT required a search and seizure. Dkt 38-2, p. 11–14. While the government disagrees with EFF's hyperbolic characterization of the government's investigation, it does not dispute that a search and seizure occurred, which is precisely why the government sought a warrant.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

experience. To begin, Playpen was no run-of-the-mill website that any internet user might just stumble upon. Rather, as a Tor hidden service, Playpen was accessible only to users who downloaded the necessary software and *knew* the precise algorithm-generated URL for Playpen. Ex. 1, p. 12, ¶ 10. This is so, the affiant explained, because "Tor hidden services are not indexed like websites on the traditional Internet" and so, "unlike on the traditional Internet, a user may not simply perform a Google search for the name of one of the websites on Tor to obtain and click on a link to the site." *Id.*

Rather, "a user might obtain the web address directly from communicating with other users of the board, or from Internet postings describing the sort of content available on the website as well as the website's location." *Id.* Indeed, the affiant noted that there is a Tor "hidden service" page dedicated to pedophilia and child pornography that contained a section with links to Tor hidden services that contain child pornography, including Playpen. *Id.* Given this, it was no great leap in logic for the magistrate to conclude that that a user who managed to find Playpen was aware of its purpose and content.

L. disagrees and points to the search engine found at https://ahmia.fi as proof that the affiant's assessment about the difficulty in finding Playpen through a traditional search was incorrect. Putting to one side that his bald assertion does nothing to undermine the conclusions of a veteran FBI agent relying on his experience and that of other experts, L. seemingly overlooks the search engine's "[c]ontent filtering policy" that states, "[w]e are removing each page which contains any child abuse from this search index" and provides a mechanism that users can report sites that contain child exploitation material. *See* https://ahmia.fi (last visited December 21, 2015).

Then, of course, there is the site itself, which the magistrate reasonably could have concluded would have immediately alerted any user to the fact that it contained illicit images. Upon arrival at Playpen's homepage, the affiant explained, the user saw "to either side of the site name . . ., two images depicting partially clothed prepubescent females with their legs spread apart. Ex. 1, p. 13, ¶ 12. The images alone are a strong

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

indicator of the presence of illicit child pornography. But there was more—namely, written underneath those suggestive images of prepubescent girls were the instructions: "[n]o cross-board reposts, .7z preferred, encrypt filenames, include preview." *Id*. While perhaps not obvious to the untrained eye, the affiant explained from his training and experience, he knew that "'no cross-board reposts'" refers to a prohibition against material that is posted on other websites from being 're-posted' to the website and '.7z' refers to a preferred method of compressing large files or sets of files for distribution." *Id.* The suggestions that filenames be encrypted and that users include previews are obvious references to the sharing of image and video files. And while such references, without more, do not compel the conclusion that the images and videos being shared are necessarily illicit, that was certainly a reasonable inference to draw, particularly given the other information available to the magistrate. Magistrates are required to be neutral, not devoid of common sense, when reviewing a warrant application.

The registration terms, to which any user who wished to log into Playpen had to agree, provide further support for the inference that Playpen's users were well aware of the its illicit purpose. As detailed above, Playpen repeatedly warned prospective users about the risks of being identified. Among other things, users were told, "the forum operators do NOT want you to enter a real [e-mail] address"; users "should not post information [in their profile] that can be used to identify [them]"; and "[t]his website is not able to see your IP." *Id.*, pp. 14-15, ¶ 13. Again, without more, these warnings may have seemed innocuous. Viewed in context, however, this focus on anonymity is entirely consistent with the desire on the part of Playpen users to avoid law enforcement detection.

Playpen's content is relevant too. As the affiant noted, upon registration, all of the sections, fora, and sub-fora were at the user's fingertips. *Id.*, p. 15, ¶ 14. The vast majority were categorized repositories for sexually explicit images of children, sub-divided by gender and the age of the victims. *Id.*, pp. 15-16, ¶ 14, n.5; *see also* Dkt. 33, Ex. D. That none of the subsections are specifically focused on adults (other than

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

perhaps the "Family Playpen – Incest" section) only reinforced the conclusion that users knew perfectly well Playpen's purpose. The affiant described in graphic detail particular child pornography that was available to Playpen users, pornography that depicted prepubescent children and even toddlers being sexually abused by adults. *Id*., pp. 17-18, ¶ 18. The affiant offered a litany of site sub-fora that contained "the most egregious examples of child pornography" as well as "retellings of real world hands on sexual abuse of children." *Id*. pp. 20-21, ¶ 27. He understandably concluded, and the magistrate reasonably found, "the entirety of [Playpen was] dedicated to child pornography." *Id.*

Courts have routinely held that membership in a child pornography website, even without specific evidence of a suspect's downloading child pornography, provides sufficient probable cause for a search warrant. This is so given the commonsense, reasonable inference that someone who has taken the affirmative steps to become a member of such a website would have accessed, received, or downloaded images from it. *See Gourde*, 440 F.3d at 1070 (finding sufficient probable cause for residential search where defendant paid for membership in a website that contained adult and child pornography; noting reasonable, commonsense inference that someone who paid for access for two months to a website that purveyed child pornography probably had viewed or downloaded such images onto his computer); *United States v. Martin*, 426 F.3d 68, 74-75 (2d Cir. 2005) (finding probable cause where purpose of the e-group "girls12-16" was to distribute child pornography; noting "[i]t is common sense that an individual who joins such a site would more than likely download and possess such material"); *United States v. Shields*, 458 F.3d 269 (3d Cir. 2006) (finding probable cause where defendant voluntarily registered with two e-groups devoted mainly to distributing and collecting child pornography and defendant used suggestive email address); *United States v. Froman*, 355 F.3d 882, 890–91 (5th Cir. 2004) ("[I]t is common sense that a person who voluntarily joins a [child pornography] group . . . , remains a member of the group for approximately a month without cancelling his subscription, and uses screen names that reflect his interest in child pornography, would download such pornography from the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

website and have it in his possession."); *accord United States v. Falso*, 544 F.3d 110 (2d Cir. 2008) (suppressing evidence from residential search for lack of probable cause where defendant was never accused of actually gaining access to the website that contained child pornography, there was no evidence that the primary purpose of the website was collecting and sharing child pornography, and defendant was never said to have ever been a member or subscriber of any child pornography site).

In short, the "numerous affirmative steps" required for a user to find and access Playpen, which made it "extremely unlikely that any user could simply stumble upon" the site "without understanding its purpose and content. Ex. 1, pp. 12-13, ¶ 10. That, combined with the information available on Playpen's homepage and registration terms, considered in light of the affiant's specialized training and experience, even in the unlikely event that someone did stumble upon Playpen, its illicit purpose would have been obvious.

2. Lorente's challenge to the magistrate's finding of probable cause utterly fails.

Nothing L. says in his motion casts doubt on the affiant's conclusions or the magistrate's finding of probable cause to deploy the NIT. Lorente's primary argument relies on a fundamental misunderstanding of the bases for the magistrate's finding of probable cause. Namely, L. claims that because, in his view, it is not readily apparent to a viewer of Playpen's homepage that the site is dedicated to child pornography, the NIT warrant must fail. For several reasons, his analysis misses the mark.

For starters, his claim that Playpen's illicit purpose was not readily apparent reflects nothing more than his disagreement with the conclusions of a seasoned FBI agent applying his considerable training and experience to objective, observable facts. As detailed above, the sexually suggestive logo, the text that accompanied it, and the registration terms all reinforced the agent's conclusion that Playpen was no mere discussion forum or a space for users to exercise their First Amendment rights as L.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

baldy asserts. Rather, he concluded Playpen was obviously a forum dedicated to the sharing of child pornography and child sexual exploitation. The Ninth Circuit has repeatedly held that "a magistrate may rely on the conclusions of experienced law enforcement officers regarding where evidence of a crime is likely to be found." *United States v. Terry*, 911 F.2d 272, 275 (9th Cir. 1990) (quoting *United States v. Fannin*, 817 F.2d 1379, 1382 (9th Cir. 1987)). This applies with equal force in child pornography cases. *See, e.g., United States v. Hay*, 231 F.3d 630, 635-36 (9th Cir. 2000) (finding affidavit that included statements based on affiant's training and experience regarding child pornography trafficking and storage provided substantial basis for probable cause determination). Moreover, officers may "draw on their own experience and specialized training to make inferences from and deductions about the cumulative information available to them that might well elude an untrained person." *United States v. Hernandez*, 313 F.3d 1206, 1210 (9th Cir. 2002) (quoting *United States v. Arvizu*, 534 U.S. 266, 273 (2002) (evaluating factors supporting reasonable suspicion)). L. is certainly free to disagree with the affiant's assessment, but his disagreement does not mean that the magistrate was compelled to do the same.

Next, that Playpen's illicit purpose was apparent was but one factor supporting the magistrate's probable cause determination. As explained in the affidavit, Playpen was no ordinary website accessible to any ordinary internet user. Access to Playpen required specialized software and knowledge of the algorithm-generated URL. L. raises the specter of the unwary internet traveler who might happen upon Playpen and login with every intention of engaging in legal conduct. But as the affiant explained, given the nature of Playpen and the "numerous affirmative steps" required to access it, such a scenario was exceedingly unlikely. Ex. 1, pp. 12-13, ¶ 10.

This is a critical observation because it is the exceedingly low probability someone would happen upon Playpen ignorant of its content that shows why the lessons he draws from *Gourde* and the other website cases do nothing advance his cause. Dkt. 33, pp. 15-19. L. takes the government to task because the NIT warrant did nothing to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

distinguish between "accidental browsers" who logged into Playpen ignorant of its illegal content and individuals seeking illegal child pornography. Dkt. 33, p. 17. *Gourde*, L. claims, stands for the proposition that membership in a website dedicated to child pornography may support a finding of probable cause so long as this illicit purpose is readily apparent to a first-time or accidental viewer. *Id.*, p. 15. Even if correct, Lorente's analysis depends on there being some chance such an "accidental browser" exists, something that Playpen, by its nature and operation, makes extremely unlikely. This conclusion finds ample support in the affidavit supporting the NIT warrant, and it was entirely reasonable for the magistrate to draw that inference and authorize the warrant. **B. L. has made no showing that justifies a *Franks* hearing, let alone established that the NIT warrant contained a material and intentional or reckless falsehood or omission.**

To be entitled to a *Franks* hearing, "the defendant must make a non-conclusory and substantial preliminary showing that the affidavit contained actual falsity [or an omission], and that the falsity either was deliberate or resulted from reckless disregard for the truth." *United States v. Prime*, 431 F.3d 1147, 1151 n.1 (9th Cir. 2005) (internal quotations omitted); *see also United States v. Meling*, 47 F.3d 1546, 1553 (9th Cir. 1995) (extending the analysis to false inclusions or omissions). A defendant must also demonstrate that the alleged falsity or omission is material. *United States v. Chavez-Miranda*, 306 F.3d 973, 979 (9th Cir. 2002). A false statement or omission is not material unless the affidavit, purged of its defects, would be insufficient to support a finding of probable cause. *Meling*, 47 F.3d at 1553; *United States v. Bennett*, 219 F.3d 1117, 1124 (9th Cir. 2000). For materiality "the pivotal question is whether an affidavit containing the omitted material would have provided a basis for a finding of probable cause." *Chavez-Miranda*, 306 F.3d at 979.

In the seminal case, *Franks v. Delaware*, the Supreme Court stressed that there is a presumption of validity with respect to a search warrant affidavit. 438 U.S. 154, 155-56 (1978). As such, under *Franks*, conclusory allegations of a defect will not do. *Id*. at 171.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

Defendants must offer allegations of intentional falsehood accompanied by an offer of proof. Affidavits or sworn or otherwise reliable statements of witnesses should be furnished or their absence satisfactorily explained before a hearing is granted. *Id*. Allegations of negligence or innocent mistake are insufficient. *Id.* In *Franks* and subsequent cases, the Supreme Court has been "careful . . . to avoid creating a rule which would make evidentiary hearings into an affiant's veracity commonplace, obtainable on a bare allegation of bad faith. It crafted, therefore, a rule of very limited scope." *United States v. Chesher*, 678 F.2d 1353, 1360 (9th Cir. 1982).

Applying these principles, there can be little doubt L. has not made anything resembling a substantial, preliminary showing of an intentional or reckless falsehood or omission. First, his offer of proof hardly suffices. He proffers no evidence that any omission of the administrator's change to the Playpen logo just before the NIT warrant was authorized was reckless, let alone intentional. Nor could he. After all, the affiant explained he had reviewed Playpen on February 18, 2015, the day before the logo changed. Ex. 1, pp. 14-15 n.3. The most that can be said is that with the benefit of hindsight, it would have been better for the affiant to have reviewed Playpen the morning the warrant was signed, as opposed to two days before. If a failing at all, which is by no means obvious, it was at worst an unintentional oversight. Indeed, it would be a stretch to characterize the agent as negligent; it certainly cannot be said he acted recklessly or with some intent to deceive. And "[m]ere negligence in checking or recording the facts relevant to a probable-cause determination is not sufficient to warrant a *Franks* hearing." *United States v. Burnes*, 816 F.2d 1354, 1358 (9th Cir. 1987) (citation and quotations omitted). Similarly, a "good faith mistake" by the affiant will not invalidate the warrant. *United States v. Botero*, 589 F.2d 430, 433 (9th Cir. 1978).

Just as important, even if that omission were intentional, it was utterly immaterial to the finding of probable cause. The administrator's replacing *two* sexually suggestive images of prepubescent girls with *one* sexually suggestive image of a prepubescent girl is hardly the game changer L. claims it is. L. derives significance from the fact

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

that, in his view, the logo and the two images that were present until the day before the NIT warrant was authorized form the *sine qua non* of the probable cause finding. That L. says it is so, however, does not make it correct. As detailed above, the magistrate's probable cause finding rested on a host of facts and inferences resting upon the affiant's specialized training and experience that demonstrated a "fair probability" that anyone who logged into Playpen did so intending view and/or share child pornography. The relevance of the image(s) in the Playpen logo was that it/they sexualized young girls. That was true before February 19, *see* Ex. 3, and it remained true after, *see* Ex. 4.

Nor do the other purported misstatements L. identifies warrant a *Franks* hearing. Indeed, much of what he characterizes as "false statements" reflect little more than his opinion about the weight the Court should attach to particular statements in the affidavit and the affiant's training and experience. For example, L. takes issue with the affiant's claim that Playpen was "dedicated to child pornography"; disputes the significance of the affiant's description of the text contained underneath those suggestive images on the website's main page; and disagrees with the affiant's assessment that accessing Playpen required "numerous affirmative steps" that made it "extremely unlikely that any user could simply stumble upon" the site "without understanding its purpose and content." Lorente's mere disagreement with the affiant's description of the facts or inferences to be drawn from those facts in light his training and experience, however, does not an omission or falsehood make.

L. is certainly free to contest whether the facts contained in the affidavit, considering the totality of the circumstances, supported probable cause. He is not, however, entitled to a *Franks* hearing simply because he does not like the inferences drawn from those facts by the affiant. And he certainly cannot convert his disagreement into a showing that the affidavit was somehow misleading just by declaring it so. Nothing in *Franks* "require[s] an affiant to provide general information about every possible theory, no matter how unlikely, that would controvert the affiant's good-faith

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

belief that probable cause existed for the search." *United States v. Craighead*, 539 F.3d 1073, 1081 (9th Cir. 2008).

Even so, beyond conclusory assertions that a particular statement is wrong or "nonsense," L. offers nothing that would suggest it constitutes an intentional or reckless falsehood. Those allegations do "not amount to the substantial showing required under *Franks*." *Meling*, 47 F.3d at 1554. "To mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine." *Franks v. Delaware*, 438 U.S. 154, 171 (1978). Lorente's remaining "*Franks*" arguments are exactly that: reflective of little more than his apparent desire to cross-examine the affiant.

L. also makes much of the fact that Playpen provided a chat forum for its members. He maintains that the affiant's characterization of Playpen as a site dedicated to child pornography swept too broadly, preventing the magistrate from considering "substantial First Amendment rights" that were implicated. Dkt. 33, pp. 22-23. It seems odd for L. to describe this as an omission given that the affiant did not omit there was a chat feature provided by Playpen. Ex. 1, pp. 19-20, ¶¶ 23-25. In any event and more importantly, the affiant also noted that even this chat feature served Playpen's illicit purpose. *Id*. In particular, the affiant provided specific examples of Playpen's chat feature being used for the purpose of distributing child pornography. *Id.*, p. 20, ¶ 25.

In short, the sum total of Lorente's *Franks* argument seems little more than a recitation of his principal argument against the finding of probable cause: that is, it was theoretically possible that a user may have accessed Playpen without the intent to view child pornography. The affiant did not claim otherwise. He merely concluded, based upon the available facts and his training and experience, that it was "extremely unlikely." Ex. 1, pp. 12-13, ¶ 10. More importantly, the magistrate agreed.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

C. The NIT warrant particularly described the locations to be searched and the things to be seized based on a showing of probable cause as to each.

The NIT warrant described the places to be searched—activating computers of users or administrators that logged into Playpen—and the things to be seized—the seven pieces of information obtained from those activating computers—with particularity. And a neutral and detached judge found that there was probable cause to support the requested search. The Fourth Amendment requires no more. Accordingly, the Court should decline Lorente's invitation to read into the Fourth Amendment a heretofore undiscovered upper bound on the number of searches permitted by a showing of probable cause.

The constitutional principles at play here are well-settled. "[N]o warrants shall issue, but upon probable cause, . . . and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const., Amend. IV. The Constitution demands that two things be described with particularity: "'the place to be searched' and 'the persons or things to be seized.'" *United States v. Grubbs*, 547 U.S. 90, 97 (2006). As to the place, it must be "described with sufficient particularity to enable the executing officer to locate and identify the premises with reasonable effort." *United States v. Turner*, 770 F.2d 1508, 1510 (9th Cir. 1985) (citations and quotations omitted). As to the items to be seized, nothing must be "left to the discretion of the officer executing the warrant" in deciding what to seize. *Marron v. United States*, 275 U.S. 192, 196 (1927). Whether this particularity standard is met is determined in light of the information available at the time the warrant issued. *United States v. Shi*, 525 F.3d 709, 731-32 (9th Cir. 2008).

The Fourth Amendment also places limits on the scope of a search. Specifically, "*what* may be seized" pursuant to a search warrant is "limited by the probable cause on which the warrant is based." *United States v. Brobst*, 558 F.3d 982, 993 (9th Cir. 2009) (emphasis added). "[T]he scope of a lawful search is 'defined by the object of the search and the places in which there is probable cause to believe that it may be found.'"

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

Maryland v. Garrison, 480 U.S. 79, 84 (1987). Therefore, "it is axiomatic that if a warrant sufficiently describes the premises to be searched, this will justify a search of the personal effects therein belonging to the person occupying the premises if those effects might contain the items described in the warrant." *United States v. Gomez-Soto*, 723 F.3d 649, 654 (9th Cir. 1984). For purposes of the Fourth Amendment, determining the proper scope of a search depends upon the relationship between the items to be seized under the warrant and the likelihood they will be found in the places to be searched.

Plainly, the NIT warrant meets both requirements. Attachments A and B of the NIT warrant, respectively, identified the "Place to be Searched" and the "Information to be Seized." Both defined with precision where agents could look and for what. The warrant authorized deployment of the NIT to the computer server hosting Playpen and then to computers of "any user or administrator who logs into [Playpen] by entering a username and password." Ex. 1, Att. A. Attachment B, in turn, imposed precise limits on what information could be obtained from those computers by the NIT:

1) the computer's actual IP address and the date and time that the NIT determines what that IP address is;

2) a unique identifier generated by the NIT to distinguish data from that of other computers;

3) the type of operating system running on the computer;

4) information about whether the NIT has already been delivered to the "activating" computer;

5) the computer's Host Name;

6) the computer's active operating system username; and

7) the computer's media access control ("MAC") address.

Tellingly, L. does not claim that the locations to be searched were not readily identifiable from the face of the warrant or that the warrant somehow left the decision of what should be seized open to debate. Nor does he claim that there is any doubt that the items authorized to be seized were not reasonably likely to be found in the places to be

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

searched. Rather, he presses a novel constitutional rule for the Internet age: the NIT warrant is an unconstitutional "general warrant" because it authorized, upon finding of probable cause, the collection of specific information from a potentially large number of computers. [5] If he is right, then hidden within the Fourth Amendment is a previously undiscovered upper bound on the number of search locations a showing of probable cause can support.

To be sure, the Fourth Amendment demands that there be probable cause to search a particular location for particular items. But the notion that a warrant supported by sufficient probable cause to authorize a search of numerous locations is, for that reason alone, constitutionally defective is absurd. Either probable cause *exists* to support a search or searches or it *does not*. Here, of course. L. maintains that the NIT warrant, which permitted the collection of information from any user or administrator who logged into Playpen, was not supported by sufficient facts to justify the search. As explained above, however, he is incorrect. There was a *fair probability* that anyone who logged into Playpen did so with knowledge of its content and the intent to consume it. Accordingly, the warrant properly authorized deployment of the NIT to any such user, regardless of how many there are or could be.

Curiously, L. finds support for his argument in the affiant's disclosure to the magistrate that although it sought authority to deploy the NIT to any user who logged into Playpen, the FBI might deploy the NIT in a more targeted fashion—*e.g.*, those users who accessed parts of Playpen containing the most egregious examples of child pornography. Ex. 1, p. 24 n.8. Lorente's point seems to be that because the FBI could execute the warrant more narrowly, it is constitutionally compelled to do so. The Fourth

---

[5] To the extent that EFF argues that the warrant in this case is comparable to a "constitutionally suspect" "all persons" warrant pursuant to *Marks v. Clarke*, 102 F.3d 1012 (9th Cir. 1996), as well as an unpublished opinion from the Southern District of Alabama and a Supreme Court opinion that EFF admits did not address the issue, its argument is unpersuasive. Dkt. 38-2, p.19–20. Significantly, in *Marks*, the Ninth Circuit explained that such a warrant may be appropriate where "there is reason to believe that all those present will be participants in the suspected criminal activity." *Id*. at 1029. As explained above, the warrant in this case laid out in detail precisely the reasons why there was probable cause to investigate any user or administrator who logged into the website.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

Amendment's particularity requirement countenances no such rule, however. A warrant is "facially deficient" only where it fails to provide any meaningful instruction to the searching agents regarding the items to be seized and "instead leaves them guessing as to their task." *United States v. Towne*, 997 F.2d 537, 549 (9th Cir. 1993). Here, the warrant authorized particular, specified information to be collected from specified users who logged in to the site with a username and password. That the FBI retained discretion to execute the warrant on a narrower set of users does not somehow convert it into an unconstitutional general warrant.

Nor do Lorente's entreaties for the Court to look to the Ninth Circuit's *CDT* decision get him anywhere. Dkt. 33, p. 25. He is correct, of course, that the Ninth Circuit has cautioned magistrates to be vigilant in approving electronic searches to strike "the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures." *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc). But the NIT warrant hardly can be described as the sort of "general exploratory search," Dkt. 33, p. 25 (quoting *United States v. Adjani*, 452 F.3d 1140, 1147-48 (9th Cir. 2006)), over which the Ninth Circuit has expressed concern. Lorente's effort to cast the NIT warrant as authorizing a sweeping electronic search of personal data strains credulity. The limited scope of the NIT warrant's authorized search is certainly relevant in assessing its reasonableness and whether the magistrate did indeed strike an appropriate balance. The NIT warrant did not subject L. to a wholesale search of his electronic devices. Rather, the NIT collected seven pieces of information that would assist law enforcement in identifying those suspected of trading and viewing child pornography.

Indeed, the most critical piece of information obtained by the NIT warrant, Lorente's IP address, is information that ordinarily would have been publicly available and over which L. cannot claim a reasonable expectation of privacy. *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2007) (Internet users have no expectation of privacy in the IP addresses of the websites they visit); *see also United States v. Suing*, 712 F.3d

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

1209, 1213 (8th Cir. 2013) (defendant "had no expectation of privacy in [the] government's acquisition of his subscriber information, including his IP address and name from third-party service providers."). Importantly, other judges in this district have expressly concluded that use of the Tor does not change things. *United States v. Michaud*, No. 3:15-CR-05351-RJB, 2016 WL 337263, at *7 (W.D. Wash. Jan. 28, 2016); *United States v. Farrell*, No. CR15-029RAJ, 2016 WL 705197, at *2 (W.D. Wash. Feb. 23, 2016); *see also* United States v. Welch, 811 F.3d 275, 278 (8th Cir. 2016)("An Internet Service Provider (ISP) assigns an IP address to an individual computer using its Internet service and associates the IP address with the physical address to which that service is being provided.")

In short, Lorente's novel rule, which he cloaks in the language of particularity and overbreadth as if to conceal its lack of constitutional foundation, cannot defeat a validly obtained warrant, supported by probable cause, that particularly describes where to search and for what. That a warrant authorizes the search of a potentially large number of suspects is an indication, not of constitutional infirmity, but a large number of criminal suspects.

D. The NIT warrant did not violate Rule 41 of the Federal Rules of Criminal Procedure, and even if it did, suppression is not an appropriate remedy.

Lorente's claim that the NIT warrant was defective under Rule 41 of the Federal Rules of Criminal Procedure also fails. First, the NIT warrant was consistent with Rule 41. Second, even if the NIT warrant somehow ran afoul of Rule 41, its use would be justified based on exigent circumstances. Finally, suppression is not an appropriate remedy for any purported violation of Rule 41.

To begin, Lorente's argument should be placed in context and its ramifications laid bare. When the government sought the NIT warrant, thousands of Playpen users were using Playpen to access and share child pornography. Playpen was set up to conceal their identities. L. does not claim the government should (or could) have sought a warrant elsewhere. He also does not suggest the government should have more

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

scrupulously hewn to the procedures for obtaining and executing a warrant contained in Rule 41. Rather, L. maintains that his use of a Tor hidden service dedicated to the sharing of child pornography means that Rule 41 denies any court in any jurisdiction power to issue a search warrant necessary to identify him. While that is certainly one way to read Rule 41, it is not the correct one.

1. Even if not explicitly authorized by Rule 41, the NIT warrant complied with the Fourth Amendment, and Rule 41 should be read broadly to permit its issuance.

Courts have long read Rule 41 broadly, interpreting it to permit searches where they are consistent with the Fourth Amendment even though not explicitly authorized by the text of the rule. In *United States v. New York Telephone Co.*, for example, the Supreme Court upheld a 20-day search warrant for a pen register to collect dialed telephone number information, despite the fact that Rule 41's definition of "property" at that time did not include information and that Rule 41 required that a search be conducted within 10 days. 434 U.S. 159, 169 & n.16 (1977). The Court explained, Rule 41 "is sufficiently *flexible* to include within its scope electronic intrusions authorized upon a finding of probable cause," and noted that this flexible reading was bolstered by Rule 57(b), which provides, "[i]f no procedure is specifically prescribed by rule, the court may proceed in any lawful manner not inconsistent with these rules or with any applicable statute." *Id.* at 169-70 (emphasis added).[6] Similarly, in *United States v. Koyomejian*, the Ninth Circuit interpreted Rule 41 broadly to allow prospective warrants for video surveillance, despite the absence of provisions in Rule 41 explicitly authorizing or governing such warrants. 970 F.2d 536, 542 (9th Cir. 1992). Nor is the Ninth Circuit unique in such an approach. As the Seventh Circuit has observed, denying courts the authority to issue warrants for searches consistent with the Fourth Amendment would encourage warrantless searches justified by claims of exigency: "holding that federal

[6] Rule 57(b) now provides: "A judge may regulate practice in any manner consistent with federal law, these rules, and the local rules of the district."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

courts have no power to issue warrants authorizing [an investigative technique] might . . . simply validate the conducting of such surveillance without warrants. This would be a Pyrrhic victory for those who view the search warrant as a protection of the values in the Fourth Amendment." *United States v. Torres*, 751 F.2d 875, 880 (7th Cir. 1984). The strong preference for reading Rule 41 broadly goes a long way to undercut Lorente's claim that the magistrate's authorization of the warrant violated that Rule.

Regardless, there was no rule 41 violation because Rule 41(b) is flexible enough to allow the issuance of warrants to investigate Tor hidden services.[7] In fact, three separate provisions of Rule 41(b) support issuance of the NIT warrant.

First, Rule 41(b)(2) allows a magistrate judge "to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed." Here, the warrant authorized use of the NIT (a set of computer instructions) located on a server in EDVA when the warrant was issued. Ex. 1, pp. 22-23, 24, ¶¶ 30, 33. As Rule 41(a)(2)(A) defines "property" to include both "tangible objects" and "information," the NIT constituted property located in EDVA when the warrant was issued. Moreover, the NIT was deployed only to registered users of Playpen who logged into the website, located in EDVA, with a username and password. *Id*., Att. A. Each of those users—including L.—accordingly reached into EDVA's jurisdiction to access the site (and the child pornography therein). Thus, Rule 41(b)(2) provided sufficient authority to issue the warrant for use of the NIT outside of EDVA.

---

[7] In order to eliminate any ambiguity on this issue, the Advisory Committee on Criminal Rules has endorsed an amendment to Rule 41 to clarify that courts have venue to issue a warrant "to use remote access to search electronic storage media" inside or outside an issuing district if "the district where the media or information is located has been concealed through technological means." *See* Advisory Committee on Rules of Criminal Rules, May 2015 Agenda, at 107-08 (available at http://www.uscourts.gov/rules-policies/records-and-archives-rules-committees/agenda-books). The amendment has been approved by the Advisory Committee on Criminal Rules, the Standing Committee, and the Judicial Conference of the United States; it is currently under review by the Supreme Court. *See* Transmittal of Proposed Amendments to the Federal Rules at 8 (available at http://www.uscourts.gov/rules-policies/pending-rules-amendments). As

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

Second, Rule 41(b)(4) specifies that a warrant for a tracking device "may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both," provided that the tracking device is installed within the district. A "tracking device" is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object." Rule 41(a)(2)(E); 18 U.S.C. § 3117(b). In a physical tracking device case, investigators might obtain a warrant to install a tracking device in a container holding contraband, and investigators might then determine the location of the container after targets of the investigation carry the container outside the district. In this case, the NIT functioned in a similar manner, except in the Internet context. Investigators installed the NIT in the Eastern District of Virginia on the server that hosted Playpen. When L. logged on and retrieved information from that server, he also retrieved the NIT. The NIT then sent network information from Lorente's computer back to law enforcement. Although this network information was not itself location information, investigators subsequently used this network information to identify and locate L.. Thus, even if Rule 41(b)(2) did not provide authority to issue the warrant, Rule 41(b)(4) did so.

Finally, the NIT warrant was issued by a judge in the district with the strongest known connection to the search: L. entered the EDVA by accessing the Playpen server there, retrieved the NIT from that server, and the NIT sent his network information back to a server in that district. The magistrate judge had authority under Rule 41(b)(1) to authorize a search warrant for "property located within the district." The use of the Tor hidden service by L. and other Playpen users made it impossible for investigators to know in what other districts, if any, the execution of the warrant would take place. In this circumstance, it was reasonable for the EDVA magistrate judge to issue the warrant. Interpreting Rule 41 to allow the issuance of warrants like the NIT warrant does not risk significant abuse because, as with all warrants, the manner of execution "is subject to later judicial review as to its reasonableness." *Dalia v. United*

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

States, 441 U.S. 238, 258 (1979). For these reasons, this Court should conclude that issuance of the warrant did not violate Rule 41.

L. cites a single magistrate judge's opinion holding that Rule 41(b) does not authorize issuance of a warrant for use of a different (and significantly more invasive) NIT than the one used in this case. *See In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013). *In Re Warrant*, though, does not undermine Magistrate Judge Buchanan's decision to issue the warrant here. The decision of one magistrate judge in one district about a different NIT could be of persuasive value, but the decision of the issuing magistrate in this case is significantly more pertinent. For starters, that case appears to be an outlier. To the government's knowledge, in every other matter involving an application for a search warrant to identify a person hiding his identity and location using Internet anonymizing techniques, the judge has issued the warrant. *See, e.g.*, *United States v. Cottom, et. al.*, No. 13-cr-108 (D. Neb. Oct. 14, 2014) (Doc #122, Attachment 1; Doc. #123, Attachment 1) (2 separate NIT search warrants), (Doc #155) (denying suppression motion); *United States v. Welch,* 811 F.3d 275 (8th Cir. 2016)(affirming denial of suppression motion in related case); *In re Search of NIT for Email Address texas.slayer@yahoo.com*, No. 12-sw-5685 (D. Col. October 9, 2012) (Doc #1) (search warrants); *In re Search of Any Computer Accessing Electronic Message(s) Directed to Administrator(s) of MySpace Account "Timberlinebombinfo" and Opening Messages Delivered to That Account by the Government*, No. 07-mj-5114 (W.D. Wash. June 12, 2007), *available at* http://www.politechbot.com/docs/fbi.cipav.sanders.affidavit.071607.pdf.

Moreover, the reasoning of the Texas magistrate judge's decision does not apply to the use of the NIT in this case. That court correctly found it "plausible" that the NIT fell within the definition of a tracking device. 958 F. Supp. 2d at 758. Nevertheless, the court held that Rule 41(b)(4) did not apply because there was no showing that the installation of the NIT software would be within its district. *See id*. That was not the case here: installation of the NIT within the meaning of Rule 41(b)(4) took place on the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

server in EDVA. As the analogy to physical tracking devices demonstrates, the government "installs" the NIT within the meaning of Rule 41(b)(4) when it adds the NIT to computer code on a computer in the issuing court's district. Lorente's subsequent retrieval of the NIT and its collection of information from his computer constituted "use of the device" for purposes of Rule 41(b)(4), regardless of whether that process of collection included "installation" on Lorente's computer.

Even if L. were correct that the warrant did not fit within the letter of Rule 41(b), the use of the NIT would nevertheless still be reasonable under the Fourth Amendment. The Supreme Court has recognized that the presumption that warrantless searches are unreasonable "may be overcome in some circumstances because '[t]he ultimate touchstone of the Fourth Amendment is 'reasonableness.'" *Kentucky v. King*, 131 S. Ct. 1849, 1856 (2011). "One well-recognized exception applies when the exigencies of the situation make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment." *Id.* (internal quotation marks omitted). The Ninth Circuit has defined exigent circumstances as "those circumstances that would cause a reasonable person to believe that entry . . . was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts." *United States v. Martinez*, 406 F.3d 1160, 1164 (9th Cir. 2005) (quoting *United States v. McConney*, 728 F.2d 1195, 1199 (9th Cir.1984) (*en banc*) (abrogated on other grounds)). Courts must evaluate "the totality of the circumstances" to determine whether exigencies justified a warrantless search. *Missouri v. McNeely*, 133 S. Ct. 1552, 59 (2013).

Here, even if the government could not obtain a warrant for use of the NIT that complied with the letter of Rule 41(b), ample exigent circumstances existed to justify its use. Playpen enabled ongoing sexual abuse and exploitation of children, and deploying the NIT against Playpen users was necessary to stop the abuse and exploitation and to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

identify and apprehend the abusers. As of early January of 2016, use of the NIT in this investigation had led to the identification or recovery from abuse of twenty-six child victims. *See* Ex. 5, pp. 7-8. The FBI also has identified at least thirty-five individuals who have been determined to be "hands on" child sexual offenders, and seventeen individuals who have been determined to be producers of child pornography. *Id*.

The information the NIT collected was also fleeting. If law enforcement had not collected IP address information at the time of user communications with Playpen, then, due to the site's use of Tor, law enforcement would have been unable to collect identifying information. Accordingly, if the warrant could not have been issued, then no warrant could have been obtained in a reasonable amount of time to identify perpetrators. *See United States v. Struckman*, 603 F.3d 731, 738 (9th Cir. 2010) (stating that to invoke the exigent circumstances exception, "the government must . . . show that a warrant could not have been obtained in time").

Moreover, the NIT warrant was minimally invasive and specifically targeted at the fleeting identifying information: it only authorized collection of IP address information and other basic identifiers for site users. Importantly, Lorente's IP address belonged to his ISP, not him, and the Ninth Circuit has held that a defendant lacks a reasonable expectation of privacy in IP addresses. *Forrester*, 512 F.3d at 510. Multiple courts in this District have held that the use of Tor does not alter that premise. *Michaud*, No. 3:15-CR-05351-RJB, 2016 WL 337263, at *7 (W.D. Wash. Jan. 28, 2016); *Farrell*, No. CR15-029RAJ, 2016 WL 705197, at *2 (W.D. Wash. Feb. 23, 2016). Before proceeding with a more invasive entry and search of Lorente's home and electronic devices, the government obtained a Rule 41 warrant issued in this district.

In sum, the NIT warrant provided authority for use of the NIT, and it is certainly preferable that the government obtain warrants (as it did here) to investigate large criminal enterprises like Playpen. Criminals' use of anonymizing technologies like Tor to perpetrate crimes should not place them beyond the reach of law enforcement (or courts). But even if no court had authority to issue a warrant to deploy a NIT to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

investigate Playpen users in Washington, as L. essentially argues is the case, its use was nonetheless reasonable under the Fourth Amendment.

2. Even if the NIT warrant violated Rule 41, the Court should not grant the extreme remedy of suppression.

Assuming *arguendo* that the warrant was somehow deficient under Rule 41, suppression is neither required by law nor reasonable under the circumstances. "Rule 41 violations fall into two categories: fundamental errors and mere technical errors." *United States v. Negrete-Gonzales*, 966 F.2d 1277, 1283 (9th Cir. 1992). "Fundamental errors are those that result in clear constitutional violations." *Id*. By contrast, technical errors may only trigger suppression upon a proper showing of prejudice or "deliberate disregard" for Rule 41. *Id*.

Suppression is a "last resort, not our first impulse," and any benefit to doing so (general deterrence of law enforcement misconduct) must outweigh the substantial social cost that results when "guilty and possibly dangerous defendants go free." *Herring v. United States*, 555 U.S. 135, 140-41 (2009). Accordingly, defendants who seek suppression must clear a "high obstacle," *id*. at 141, and "resolution of doubtful or marginal cases … should largely be determined by the preference to be accorded to warrants." *United States v. Kelley*, 482 F.3d 1047, 1050-51 (9th Cir. 2007) (citing and quoting *Illinois v. Gates*, 462 U.S. 213, 237 n.10 (1983)).

In the Rule 41 context in particular, the Ninth Circuit has observed, "we have repeatedly held—and have been instructed by the Supreme Court—that suppression is rarely the proper remedy for a Rule 41 violation." *United States v. Williamson*, 439 F.3d 1125, 1132 (9th Cir. 2006). "Because the exclusionary rule tends to exclude evidence of high reliability, the suppression sanction should only be applied when necessary and not in any automatic manner." *United States v. Luk*, 859 F.2d 667, 671 (9th Cir. 1988) (affirming denial of suppression motion despite a technical violation of Rule 41). Whether exclusion is warranted "must be evaluated realistically and pragmatically on a

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

case-by-case basis." *Id*. (*quoting United States v. Vasser*, 648 F.2d 507, 510 n.2 (9th Cir. 1981), *cert. denied*, 450 U.S. 928 (1981)).

None of the three bases L. alleges warrant suppression withstand scrutiny. First, there was no violation of constitutional magnitude. L. wrongly claims that jurisdictional flaws and other fundamental violations of non-ministerial requirements necessarily involved matters of constitutional magnitude. Dkt. 33, p. 37. He is wrong. He offers no explanation as to how use of the NIT represented a "clear constitutional violation." *See United States v. Johnson*, 660 F.2d 749, 753 (9th Cir. 1981) (requiring a showing that the search was "unconstitutional under traditional fourth amendment standards"). No surprise here because there were none. The Ninth Circuit has made clear that a "paradigmatic example" of a constitutional violation is where *no* warrant is sought. *Luk*, 859 F.2d at 673 (*citing United States v. Alvarez*, 810 F.2d 879 (9th Cir 1987)). In *Alvarez*, the court reversed the defendant's conviction because the district court did not order suppression after the government arrested the defendant in a non-public place without a warrant despite having sufficient time to obtain one telephonically pursuant to then-Rule 41(c)(2). 859 F.2d at 882-84. That is clearly not the case here. Courts have also repeatedly declined to find a constitutional violation based on a claim that "a warrant" was issued "by an unauthorized judge"—which seems to be Lorente's concern here. *Luk*, 859 F.2d at 673 (collecting cases). Lorente's Rule 41 argument takes issue with the government's chosen forum for obtaining the warrant, not the constitutional soundness of the warrant itself or its execution. The government's error in choosing a forum, if it indeed it were an error, is thus not one of constitutional import.

As important, the search and seizure here complied with the Fourth Amendment. The Fourth Amendment demands three things of a search warrant: a warrant must be issued by a neutral magistrate; it must be based on a showing of "probable cause to believe that the evidence sought will aid in a particular apprehension or conviction for a particular offense"; and it must satisfy the particularity requirement. *Dalia*, 441 U.S. at 255. As detailed above, the NIT warrant easily meets these requirements.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

The government's actions here were also reasonable under the circumstances. Law enforcement has a substantial interest in identifying users of a massive website trafficking in child pornography. The court-authorized use of the NIT was necessitated by the Tor-based technology L. and other offenders under investigation used to exploit children, which made it impossible for investigators to know where he was located without first using the NIT. *Id.*, p. 23-24, ¶ 31. The individual privacy interests here were extremely limited, due to the minimally invasive nature of the NIT search and its focus on IP address information over which L. lacks a reasonable expectation of privacy. *See Forrester*, 512 F.3d 500 (Internet users have no expectation of privacy in the IP addresses of the websites they visit); *see also Suing*, 712 F.3d 1209, 1213 (8th Cir. 2013) (defendant "had no expectation of privacy in [the] government's acquisition of his subscriber information, including his IP address and name from third-party service providers."). Courts must weigh those privacy interests against "the needs of law enforcement," such as the "need for flexibility that allows police to do their job effectively." *United States v. Martinez-Garcia*, 397 F.3d 1205, 1211 (9th Cir. 2005). The very fact the government sought and obtained a warrant from a neutral magistrate protected L. from an unreasonable search and seizure in violation of his constitutional rights. *See Alvarez*, 810 F.2d at 883 (interposing magistrate between law enforcement and target protects against unreasonable searches and seizures). Obtaining that warrant from a magistrate judge in the district where the website was hosted and where users like L. went to retrieve information from the website was eminently reasonable, particularly given the lack of available options.

Next, L. wrongly argues that he suffered such prejudice that suppression is necessary. Dkt. 33, pp. 35-36. However, any deviation from the letter of Rule 41 was the product of Playpen's users (including L.) using Tor to evade law enforcement,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

not some bad faith on the part of law enforcement in trying to comply with Rule 41.[8] The Ninth Circuit has found no prejudice to exist from a Rule 41 violation where "the circumstances under which the warrant was sought at least partially justified the agents' deviation from the letter of the Rule" and a warrant "complies with the spirit of Rule 41 in that it provided a basis for a probable cause determination and established an adequate record to review that determination." *United States v. Vassar*, 648 F.2d 507, 510 (9th Cir. 1980). As Judge Bryan found in *Michaud*, any Rule 41 infraction ran counter to the letter, but not certainly the spirit, of Rule 41. *Michaud*, 2016 WL 337263 at *6.

Nor has L. presented a credible argument about why he was prejudiced. He first claims that had the FBI complied with the warrant, it would have only searched computers in the Eastern District of Virginia, and not Washington. Dkt. 33, p. 35. That argument ignores the pertinent facts. The use of Tor by L. and other Playpen users made it impossible for the FBI to identify their true location before deploying the NIT to reveal their true IP addresses and, through further investigation, their true locations. If, as L. argues, Rule 41 authorized the NIT to be deployed to users in the Eastern District of Virginia, then the search of Lorente's computer still would have occurred—because the user's location was unknown until after the search. In other words, Lorente's computer would still have been searched had, in his view, the Rule been followed.

Next, L. claims that if the warrant did indeed authorize a search of his computer in Washington, then the prejudice was that the warrant violated Rule 41. Dkt. 33, p. 35. But this is simply a re-articulation of the argument that any violation of Rule 41, no matter how small, constitutes sufficient prejudice to warrant suppression. The Ninth Circuit specifically rejected that argument in *Vassar*, 648 F.2d at 510 n.2, as did Judge Bryan in *Michaud*, 2016 WL 337263 at *6-7.

---

[8] As Judge Bryan found, "[t]he rule does not directly address the kind of situation that the NIT warrant was authorized to investigate, namely, where criminal suspects geographical whereabouts are unknown, perhaps by design, but the criminal suspects had made contact via technology with the FBI in a known location." *Michaud*, No. 3:15-CR-05351-RJB, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

At its core, Lorente's argument is that no court anywhere could have issued a warrant to permit a search of his computer because the server hosting Playpen was situated in a different district and he used Tor to hide his location. That is not the sort of claimed "prejudice" that should result in suppression. Having already used Tor to shield his location from investigators, under no reasonable analysis should L. be permitted to wield it as a sword to defeat the government's ability to obtain judicial authorization to search for the true location from which he accessed child pornography. "The policies behind the exclusionary rule are not absolute and must be evaluated realistically and pragmatically on a case by case basis." *Vassar*, 648 F.2d at 510 n.2. Nor should this court "fault the good faith ingenuity of the officers" in responding to the defendant's use of advanced technology with its own, where "interests protected by the fourth amendment and Rule 41 were safeguarded by the officers . . . even though the methods used were novel." *Id*.

Indeed, had L. not concealed his true location, the government could have obtained a search warrant from a magistrate judge in this district. *See United States v. Weiland*, 420 F.3d 1062, 1071 (9th Cir. 2005) (rejecting claim of prejudice where law enforcement officer could have obtained warrant from a separate judicial officer); *Johnson*, 660 F.2d at 753 (same). In any event, as noted above, the government nonetheless could have proceeded with the NIT search without a warrant, due to the exigent circumstances created by Lorente's use of the Tor network to conceal his location and identity.

Lorente's reliance on cases such as *United States v. Krueger* and *United States v. Glover* does not alter this. Those cases involved searches of a residence and a car whose precise physical location were known to be located outside of the magistrates' districts when the warrants were issued. *See Krueger*, 998 F. Supp. 2d 1032, 1034-35 (D. Kan. 2014); *Glover*, 736 F.3d 509, 510 (D.C. Cir. 2013). Appropriate warrants, it stands to reason, could have been obtained from judges in the districts where the residence and car were located. The lessons of those cases have little to offer here.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

Finally, suppression is not warranted, as L. alleges, because the government intentionally and deliberately disregarded Rule 41's jurisdictional limitations. Dkt. 33, pp. 38-39. In the Ninth Circuit, suppression is only warranted in the case of a deliberate violation of Rule 41 if that violation occurs in "bad faith." *See Luk*, 859 F.2d at 673 ("suppression is required for nonfundamental violations in bad faith"); *see also Williamson*, 439 F.3d at 1134 ("Other cases have equated 'deliberate and intentional disregard' with 'bad faith.'"). As in *Luk*, the warrant request here was the product of a lengthy investigation by agents who, rather than attempting to avoid compliance with Rule 41, deliberately sought to satisfy the letter of Rule 41 by seeking a warrant in the district with the greatest known connection to the criminal activity. *See* 859 F.3d at 675 (describing investigation). There is no evidence that agents hid critical information from the magistrate or otherwise prevented the magistrate from having all the necessary information. This case is hardly analogous to cases such as *United States v. Gantt*, where the Ninth Circuit affirmed suppression because agents deliberately and without justification failed to provide an individual with a copy of a warrant as required by Rule 41(d). 194 F.3d 987, 994-95 (1999). Rather, law enforcement reasonably concluded that under Rule 41, an EDVA judge could issue a warrant to deploy a NIT on a server in EDVA which would be activated only after individuals—who had undertaken conscious efforts to conceal their location—voluntarily entered EDVA to access the server. Even if that conclusion were erroneous, such a misapprehension can hardly be taken as evidence of "bad faith." Accordingly, suppressing highly probative evidence that agents used to identify L. is unjustified. *See Williamson*, 439 F.3d at 1134 ("[W]here the agent executing the warrant is unaware of the Rule but acts in good faith in executing what he or she believes to be the Rule, he or she has not acted in deliberate disregard of it; thus suppression is not appropriate.").

L. nonetheless insists that the government committed an intentional violation of Rule 41, pointing to the government's proposal and support of an amendment to Rule 41. The proposed amendment to Rule 41 was intended to clarify that courts have venue

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

to issue a warrant "to use remote access to search electronic storage media" inside or outside an issuing district if "the district where the media or information is located has been concealed through technological means." This proposed amendment and the accompanying letter from the then Assistant Attorney General for the Criminal Division of the Department of Justice prove the government recognized the need for clarification. They do not reflect a concession that but for that clarification, Rule 41 is a bar to the approach taken by the government in this case. That the Department of Justice seeks greater clarity in the rule does not convert conduct taken in good faith to a deliberate and intentional violation of the rule. Moreover, at the time the Department of Justice proposed the Rule 41 Amendment, a single magistrate judge in one case had rejected a warrant to locate a computer concealed through technological means, but every other magistrate judge known to consider the issue had issued such a warrant.

E. None of Lorente's other claimed defects in the NIT warrant justify the extraordinary remedy of suppression.

None of the remaining flaws in the NIT warrant L. identifies justify the extraordinary remedy of suppression. First, Lorente's claim that the NIT warrant was void because, as an anticipatory warrant, the "triggered event" never occurred is little more than a rehash of same probable cause and *Franks* challenges that have already been addressed. Next, his claim that the NIT warrant did not authorize deployment of the NIT to his computer because it was located in Washington relies on an obtuse and crabbed reading of the authorizing warrant and its attachments that this Court should not endorse. The FBI sought authority to deploy the NIT to activating computers, wherever located, and that is exactly what it did. Finally, L. is not entitled to a suppression remedy as an alternative to his request for dismissal.

1. The NIT warrant was a valid anticipatory warrant.

Although L. does not appear to challenge the notion that the NIT warrant could be categorized as an anticipatory warrant, he wrongly asserts that it was void

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

because the "triggering event" that would authorize its execution against him never occurred. Dkt. 33, pp. 26-28.

It is well-settled that the Fourth Amendment is no bar to "anticipatory warrants." These warrants are "no different in principle from ordinary warrants." *United States v. Grubbs*, 547 U.S. 90, 96-97 (2006). "[T]wo prerequisites of probability must be satisfied. It must be true not only that if the triggering condition occurs 'there is a fair probability that contraband or evidence of a crime will be found in a particular place,' but also that there is probable cause to believe the triggering condition will occur." *Id.*

Here, the relevant "triggering event" was Lorente's decision to enter his username and password into Playpen and enter the site. (Although as was the case with many other users, the NIT was not deployed to L. immediately upon login but once he accessed a particular section of the site.) And here too, the NIT warrant affidavit provided ample support for the probable cause determination as to both. Attachments A and B, which were incorporated into the warrant, specified the exact conditions under which the NIT was authorized to be deployed–*i.e.*, when a user such as L. logged into Playpen—and as discussed in detail above, there was probable cause to believe that any user who logged onto Playpen was seeking child pornography.

L. posits that because this "triggering event" never occurred, the NIT warrant was void. Notably, he is not claiming that L. did not in fact log into Playpen. Instead, Lorente's argument on this point is just a recitation of his probable cause and *Franks* challenges. As noted above, there was ample support for the magistrate's finding of probable cause, and L. utterly fails in his effort to make out a *Franks* challenge to the warrant. Accordingly, his claim about the absence of a "triggering event" to support execution the NIT warrant must also fail.

2. The NIT warrant plainly authorized deployment of the NIT to Lorente's computer.

The NIT warrant, read in full, plainly authorized the deployment of the NIT to Lorente's computer notwithstanding the fact that it was physically located in Washington

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

State. The warrant and accompanying attachments made clear to the magistrate that the NIT was to be deployed initially to the web server hosting Playpen in the Eastern District of Virginia and then obtain information from computers that logged into Playpen, wherever they may be located.

No one, including the authorizing magistrate, could have thought otherwise. For starters, the warrant application and warrant are captioned "in the matter of the search of computers that access [the URL of Playpen]." Moreover, Attachment A to the warrant provided:

> This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below.
>
> The computer server is the server operating the Tor network child pornography website referred to herein as the TARGET WEBSITE, as identified by its URL -upf45jv3bziuctml.onion - which will be located at a government facility in the Eastern District of Virginia. The activating computers are those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password.

The affidavit also left no room for doubt that the location of the activating computers was unknown and that the purpose of deploying the NIT was to aid in identifying their location. For instance, the affiant explained that without the use of the NIT, "the identities of the administrators and users of [Playpen] would remain unknown." Ex. 1, p. 22, ¶ 29; *see also id.*, pp. 23-34, ¶¶ 31-32 ("[U]sing a NIT may help FBI agents locate the administrators and users" of Playpen.); *Id.*, p. 23, ¶ 31 (noting the NIT was a "presently available investigative technique with a reasonable likelihood of securing the evidence necessary to prove . . . the actual location and identity" of Playpen users "engaging in the federal offenses enumerated."). Finally, the affiant specifically requested authority for the NIT to "cause an activating computer—wherever located—to send to a computer controlled by or known to the government . . . messages containing

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

information that may assist in identifying the computer, its location, other information about the computer and the user of the computer." *Id*., pp. 29-30, ¶ 46(a).

In terms of the deployment of the NIT, the affidavit explained that the NIT consisted of additional computer instructions that would be downloaded to a user's computer along with the other content of Playpen that would be downloaded through normal operation of the site. *Id.*, p. 24, ¶ 33. Those instructions, which would be downloaded from the website located in the Eastern District of Virginia, would then cause a user's computer to transmit specified information to a government-controlled computer. *Id*. The affidavit specifically requested authority to deploy the NIT to any user who logged into Playpen with a username and a password. *Id*., p. 26, ¶ 36.

The only fair reading of the NIT warrant, application, affidavit, and attachments leads to one conclusion: the government sought authority to deploy the NIT to any computer that entered the Eastern District of Virginia and logged into Playpen, regardless of the physical location of that computer.

Lorente's self-serving and myopic insistence that the Court confine its inquiry to text in the face sheet of the warrant is understandable but unsupportable. And it certainly does not justify suppression.

3. Suppression is not warranted as a lesser sanction for the government's alleged misconduct.

Pointing to his motion to dismiss, Dkt. 30, L. makes his last stand in his fight for suppression, suggesting that even if dismissal is not an appropriate remedy for the government's actions, suppression is. Dkt. 33, p. 4. He is wrong. L. offers no authority suggesting that suppression would be justified by the so-called misconduct he has identified. That alone should end the inquiry. But as detailed in the government's response to Lorente's motion to dismiss, the government's conduct in this investigation was not even unreasonable, let alone outrageous.

Although Lorente's request for suppression as a lesser sanction argument fails, two points he raises merit a brief response. First, he claims the government should be

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

punished for its lack of candor with the Court, seemingly an allusion to his unsupported assertion that the FBI withheld from Magistrate Judge Buchanan its intention to operate Playpen for a period of time. As noted above, there was no such concealment. *See* Ex. 1, p. 23, ¶ 30.

Second, L. seeks to bolster his criticism of the government's investigation by observing that the FBI's seizure and takeover of Playpen "was illegal, since there are no statutory or other legal exemptions that allow law enforcement to publicly disseminate child pornography." Dkt. 33, p. 4. The absence of express statutory authorization, however, can likely be explained by the unremarkable and commonsense principle that where law enforcement officers take actions within the scope of their duties to investigate criminal conduct, a criminal statute that might otherwise render such conduct illegal "shall be construed to exempt the government" where its "application to the government would create an absurdity." *United States v. Mack*, 164 F.3d 467, 472 (9th Cir. 1999) (citing *Nardone v. United States*, 302 U.S. 379, 383-84 (1937)). In order to enforce criminal child pornography laws and prosecute defendants, law enforcement officers obviously must view, download, receive, and possess child pornography—all actions that would otherwise be illegal. Surely, Lorente's argument to the contrary is exactly the sort of absurdity the Ninth Circuit had in mind in *Mack*.

Lorente's dissatisfaction with having been discovered through the NIT is understandable. But the mere fact that he objects to having been unmasked, without more, does not support a finding of government misconduct. And it certainly does not warrant suppression of evidence obtained pursuant to a warrant issued by a neutral and detached magistrate based on a finding of probable cause.

F. Even if the warrant does not satisfy the Fourth Amendment or Rule 41, the good faith exception bars suppression here.

Under the good faith exception to the Fourth Amendment's exclusionary rule, suppression is not warranted where officers rely in good faith on an objectively reasonable search warrant issued by a neutral and detached judge. *United States v. Leon*,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

468 U.S. 897, 900 (1984). This objective standard is measured by "whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." *Id.* at 922 n.23. "[A] warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search." *Id*. at 922 (quotation marks omitted). The Supreme Court observed that "suppression of evidence obtained pursuant to a warrant should be ordered only on a case-by-case basis and only in those unusual cases in which exclusion will further the purposes of exclusionary rule." *Id.* at 918. The Court identified only four circumstances where exclusion is appropriate. Those are where: (1) the issuing magistrate was misled by the inclusion of knowing or recklessly false information; (2) the issuing magistrate wholly abandoned the detached and neutral judicial role; (3) the warrant is facially deficient as to its description of the place to be searched or the things to be seized; or (4) the affidavit upon which the warrant is based is so lacking in indicia of probable cause that no reasonable officer could rely upon it in good faith. *Id.* at 923-24. None apply here.

Here, the warrant affidavit contained no knowingly or recklessly false information that was material to the issue of probable cause. Nor does L. allege that the issuing magistrate abandoned her judicial role. The warrant clearly and particularly described the locations to be searched and the items to be seized. And the affidavit made a strong, comprehensive showing of probable cause to deploy the NIT. Absent any of these errors, once the magistrate signed the warrant after having been made aware of how the NIT would be implemented and its reach, the agents' reliance on that authority was objectively reasonable. *See Massachusetts v. Sheppard*, 468 U.S. 981, 989-90 (1984) ("[W]e refuse to rule that an officer is required to disbelieve a judge who has just advised him, by word and by action, that the warrant he possesses authorizes him to conduct the search he has requested").

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

The same holds true for any alleged Rule 41 infirmity. *See Negrete-Gonzales*, 966 F.2d at 1283 (applying good faith doctrine in the context of a Rule 41 violation).[9] "The Supreme Court's goal in establishing the good-faith exception was to limit the exclusionary rule to situations where the illegal behavior of officers might be deterred." *United States v. Gantt*, 194 F.3d 987, 1006 (9th Cir. 1999).

The actions at issue here hardly come close to constituting "illegal behavior" or "police misconduct," *id.*, warranting the extreme remedy of suppression. For starters, law enforcement sought a warrant from a neutral and detached judge to deploy the NIT, which the Ninth Circuit recognizes as "the most fundamental policy of the Rule." *Luk*, 859 F.2d at 674. Moreover, it supported its request with a 31-page affidavit that spelled out in detail the abundant probable cause justifying deploying the NIT, the location-obscuring technology L. and others used to evade law enforcement and disseminate child pornography, the fact that the NIT would reach computers wherever they might be, and the limited pieces of information the NIT would retrieve. Further, law enforcement sought this authorization from the district where Playpen would operate and in which L. and others would enter to access the site. To the extent no other district was available, that was purely due to the purposeful use of sophisticated technology by L. and others to mask their true location. Accordingly, any jurisdictional flaw under Rule 41 was the product of a good faith effort to identify an appropriate venue, consistent with Rule 41, from which to seek a warrant, not an effort to circumvent the Rule's requirements. Under these circumstances, the officers' reliance on the warrant was objectively reasonable, regardless of any flaws it may have had, and the good faith exception precludes suppression. *Gantt*, 194 F.3d at 1005 ("If the executing officers act in good faith and in reasonable reliance upon a search warrant, evidence which is seized under a facially valid warrant which is later held invalid may be admissible.") (quotation marks omitted); *see also Sheppard*, 468 U.S. at 987-88. Ultimately, agents acted

[9] To the extent L. questions whether the good faith exception applies post-*Weiland*, that court had no opportunity to address this issue as it found that suppression was not warranted. 420 F.3d at 1071 (9th Cir. 2005).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7790

reasonably in relying upon the magistrate's authorization of the NIT warrant, and so the evidence seized pursuant to it should not be suppressed.

IV. CONCLUSION

For all the foregoing reasons, the Court should deny Lorente's motion to suppress evidence.

DATED this 7th day of March, 2016.

Respectfully submitted,

ANNETTE L. HAYES
United States Attorney

/s/ Matthew P. Hampton
Matthew P. Hampton
Andre M. Penalver
Assistant United States Attorney
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402
Telephone: (253) 428-3800
Fax: (253) 428-3826
E-mail: matthew.hampton@usdoj.gov
andre.penalver@usdoj.gov

STEVEN J. GROCKI
Chief

/s/ Keith A. Becker
Trial Attorney
Child Exploitation and Obscenity Section
1400 New York Ave., NW, Sixth Floor
Washington, DC 20530
Phone: (202) 305-4104
Fax: (202) 514-1793
E-mail: keith.becker@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on March 7, 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 the attorney(s) of record for the defendant.

s/Emily Miller
EMILY MILLER
Legal Assistant
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
Phone: (206) 553-2267
FAX: (206) 553-0755
E-mail: emily.miller@usdoj.gov