UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA,

Plaintiff,

v.

ALEX LEVIN,

Defendant.

Case No. 15-CR-10271-WGY

UNDER SEAL

GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTION TO SUPPRESS

The United States of America, by and through its undersigned attorneys, respectfully submits this response to the defendant's motion to suppress. The defendant, Alex Levin, filed a motion to suppress evidence obtained via two court-authorized search warrants issued upon findings of probable cause by two neutral and detached magistrates. He does not challenge any of the assertions in any of the warrants. Rather, the defendant contends that the first of those search warrants was improperly issued which, he asserts, should result in suppression of all evidence seized pursuant to the warrants. His arguments are unavailing. The warrants were amply supported by probable cause to investigate the registered users of a massive child pornography website whose users, including the defendant, deployed advanced technological measures to hide their identity and location while they exploited children. Moreover, suppression is particularly inappropriate here, where law enforcement officers acted in good-faith reliance upon the issuance of those warrants and in compliance with FED. R. CRIM. P. 41. Accordingly, for the reasons set forth more fully below, the United States requests that this Court deny the motion to suppress.

I. BACKGROUND

The charges in this case arise from an investigation into a global online forum dedicated to the advertisement and distribution of child pornography through which registered users like the defendant regularly advertised, distributed and accessed illegal child pornography.[1] The scale of child sexual exploitation that occurred on the site was massive – it contained more than 150,000 total members who collectively engaged in tens of thousands of postings related to child pornography. The images and videos that were advertised, distributed and accessed through the site were highly categorized according to the gender and age of the victims portrayed – including so-called "jailbait," "pre-teen" and "toddlers;" as well as the type of sexual activity depicted – including hardcore ("HC") and softcore ("SC") child pornography. The most postings to the site (more than 20,000 posts) were made within a sub-section for "Pre-teen" videos dubbed "Girls HC," where hardcore pornographic images of pre-teen girls were advertised, distributed and accessed. The site also contained forums for the discussion of matters pertinent to child sexual abuse, including methods and tactics offenders use to abuse children, as well as methods and tactics offenders use to avoid law enforcement detection while perpetrating online child sexual exploitation crimes. It did not advertise or distribute adult pornographic images.

The site, referenced herein as "Website A," operated on the anonymous Tor network – which allows users to mask their actual IP addresses while accessing the Internet.[2] In order to

[1] In order to protect the security of the ongoing investigation, the actual name of the website was not disclosed in pertinent search warrant documents, but was alternately referenced as the "TARGET WEBSITE" or "Website A." It is referenced herein as "Website A."

[2] Tor was originally designed, implemented, and deployed as a project of the U.S. Naval Research Laboratory for the primary purpose of protecting government communications. It is now available to the public at large. Information documenting what Tor is and how it works is provided on the publicly accessible Tor website at www.torproject.org. Owed to its anonymizing properties, the Tor network has become 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 October 15, 2015).

access the Tor network, a user must install Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle" available at www.torproject.org.[3] Use of the Tor software masks the user's actual IP address, which could otherwise be used to identify a user, by bouncing user communications around a distributed network of relay computers (called "nodes") run by volunteers all around the world. Because of the way Tor routes communications through other computers, traditional IP-address-based identification techniques used by law enforcement agents investigating online crimes are not viable. When a user on the Tor network accesses a website, for example, the IP address of a Tor "exit node," rather than the user's actual IP address, shows up in the website's IP log. An exit node is the last computer through which a user's communications were routed. Tor is designed to prevent tracing the user's actual IP address back through that Tor exit node IP address.

Within the Tor network itself, entire websites, such as "Website A," can be set up as "hidden services." "Hidden services," like other websites, are hosted on computer servers that communicate through IP addresses and operate the same as regular public websites with one critical exception. The IP address for the web server is hidden and instead is replaced with a Tor-based web address, which is a series of algorithm-generated characters, such as "asdlk8fs9dflku7f" followed by the suffix ".onion." A user can only reach these "hidden services" if the user is using the Tor client and operating in the Tor network. And unlike an open Internet website, is not possible to determine through public lookups the IP address of a computer hosting a Tor "hidden service." Neither law enforcement nor users can therefore determine the location of the computer that hosts the website through those public lookups.

The use of the Tor network also makes websites like "Website A" more difficult to find

[3] Users may also access Tor through so-called "gateways" on the open Internet, however, use of those gateways does not provide users with the full anonymizing benefits of Tor.

for users. Even after connecting to the Tor network, a user must know the exact web address of a site like "Website A" in order to access it. Accordingly, in order to find "Website A," a user had to first obtain the web address for it from another source – such as from other users of "Website A," or from online postings describing both the sort of content available on "Website A" and its location. Accessing a Tor website like "Website A" therefore required numerous affirmative steps by the user, making it extremely unlikely that any user could have simply stumbled upon "Website A" without first understanding its content and knowing that its primary purpose was to advertise and distribute child pornography.

While the FBI was able to view and document the substantial illicit activity taking place on "Website A," investigators faced a tremendous challenge to identify the site users engaging in the sexual exploitation of children through the site. Open-Internet, non-Tor websites generally have user IP address logs that can be used to locate and identify the site's users. In such cases, after the lawful seizure of a website whose users were engaging in unlawful activity, law enforcement could review those IP logs in order to determine the IP addresses of site users. Law enforcement agents could then perform a publicly available lookup to determine what Internet Service Provider ("ISP") owned the target IP address, and address a subpoena to that ISP to determine the user to which the IP address was assigned at a pertinent date and time. However, because Website A was a Tor website, any such logs of user activity would contain only the IP addresses of the last computer through which the communications of Website A users were routed before the communications reached their destinations. The last computer is not the actual user who sent the communication or request for information, and it is not possible to trace such communications back through the Tor network to that actual user. Such IP address logs therefore could not be used to locate and identify users of Website A. Accordingly, in order for

law enforcement to be able to attain the sort of information that would normally be available from public sources and through ordinary investigative means, the offenders' use of the Tor network necessitated a particular investigative strategy.

Acting on a tip from a foreign law enforcement agency as well as further FBI investigation, the FBI determined that the computer server that hosted Website A was located at a web-hosting facility in North Carolina. In February of 2015, FBI agents apprehended the administrator of Website A and seized the website from its web-hosting facility in North Carolina. Rather than merely shut the site down, which would have allowed the users of the site to go unidentified (and un-apprehended), the FBI interdicted the site and allowed it to continue to operate at a government facility located in the Eastern District of Virginia during a two-week period between February 20, 2015, and March 4, 2015. During that brief period, the FBI obtained court approval from the United States District Court for the Eastern District of Virginia to monitor site users communications and to deploy a Network Investigative Technique ("NIT") on the site, in order to attempt to identify registered site users who were anonymously engaging in the continuing sexual abuse and exploitation of children, and to locate and rescue children from the imminent harm of ongoing abuse and exploitation.[4] As described in detail in the application for the warrant authorizing its use, the NIT consisted of computer instructions which, when downloaded (along with the other content of Website A) by a registered user's computer, were designed to cause the user's computer to transmit a limited set of information – the computer's true IP address and other computer-related information – that would assist in identifying the computer used to access Website A and its user. Ex. 1, pp. 23-27, ¶¶ 31-37. The search warrant authorization permitted that minimally invasive technique to be deployed when a registered user logged into Website A by entering a username and password, while the website

[4] The NIT search warrant, affidavit and return (No. 15-SW-89) are attached as Exhibit 1.

was located in the Eastern District of Virginia. *Id.*, p. 24, ¶ 32; p. 23, Att. A.[5]

On August 11, 2015, law enforcement agents obtained from this District (Magistrate Judge Marianne B. Bowler) a search warrant for the defendant's home.[6] The warrant described Website A in detail and articulated that data obtained from logs on "Website A," court-authorized monitoring by law enforcement, and the court-authorized deployment of a NIT, had revealed that Website A user "Manakaralupa" accessed child pornography on the site on March 4, 2015. Ex. 2, p. 11, ¶¶ 25-26. Specifically, on March 4, 2015, the user "Manakaralupa" with IP address 108.20.181.106 accessed a forum entitled, "Strawberry Shortcake Reuped on 03/04/2015." Among other things, this post contained a link to an image (.jpg file) of a photo collage that depicted a pre-pubescent female, about five to seven years old, posed in a variety of poses in which the focal point of some of the photos was the child's vagina, anus, and one that had a penis placed against her mouth. On the same date, the user "Manakaralupa" accessed a file entitled "Estefy (Latina Anal) Deep anal creampie - asi se mama linda.3gp." The file contained one image that contained a collage of images of a prepubescent female performing oral sex and anal sex with an adult male. I*d.* The NIT determined the IP address of that user, which according to a publicly available website belonged to Verizon. *Id.*, p. 12, ¶ 28. Information furnished by Verizon in response to an FBI subpoena tied the IP address collected by the NIT for that user to the defendant's home. *Id.*, 12, ¶¶ 29-30.

On August 12, 2015, agents executed that warrant and searched the defendant's home, pursuant to which agents located a computer that had contained child pornography. A forensic

[5] The NIT affidavit explained that, in order to ensure technical feasibility and avoid detection of the technique by subjects of investigation, the FBI would deploy the technique more discretely against particular users, such as those who attained a higher status on the website by engaging in substantial activity, or in particular areas of the website, such as those with the most egregious examples of child pornography, which sub-forums were described in the affidavit. Ex. 1, pp 24-25, ¶ 32, n. 8.

[6] The residential search warrant application, and affidavit (No. 15-MJ-2187-MBB) are attached as Exhibit 2.

review of the computer revealed seven videos and one still image, all of which constitute child pornography. The seven videos containing child pornography included the following:

0-2010 pthc babyshivid frifam 5yo sally gets fucked by day (very excellent).avi – this video, which is 1 minute 20 seconds in duration, features a series of sexual encounters between a nude prepubescent female child and a nude adult male, including the adult male inserting his penis into the child's vagina. The video also depicts the naked female child inserting or rubbing two "dildos" against her vaginal and anal areas.

0-kiddy porn (asian lolita) 0708 – cambodian girl (11 yo) fucks 10 yo girl and man (excellent, pthc).mpg – this video, which is 11 minutes 26 seconds in duration, depicts a prepubescent female being vaginally penetrated by an adult's penis, as well as a prepubescent female inserting a "dildo" into the vagina of a second prepubescent female.

0_t-169754455-bibcam-pjk-pthc-kdv-rbv-pedo---01---sk—starskysh---boys-13yo-1.mpg - This video, which is 15 minutes 4 seconds in duration, depicts two boys approximately 13 years of age masturbating and performing oral sex.

The forensic examination of the computer revealed that the above-described three child pornography videos were each saved to his computer on October 11, 2011, at 8:59 p.m., 9:33 p.m., and 9:34 p.m. respectively.

On September 17, 2015, the defendant was indicted on one count of possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). On or about February 18, 2016, the defendant filed a motion to suppress the EDVA NIT warrant and all information seized pursuant to it, and the residential search warrant.

II. SEARCH WARRANT AUTHORIZING THE NIT

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 law enforcement in identifying registered site users who were utilizing anonymizing technology to expose children to ongoing and pervasive sexual exploitation on a massive scale.

A. Technical and Legal Background of Investigation

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 iterating 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 Website A. *Id.*, pp. 10-13, ¶¶ 7-10. The affidavit specified the numerous steps a user would have to go through just in order to find Website A, because it was a Tor hidden service, and not an ordinary website. In particular, the affidavit noted that:

> 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. [Website A] is listed in that section.

Id., pp. 12-13, ¶ 10. The experienced affiant accordingly opined that: "Accessing the TARGET WEBSITE therefore requires numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble upon the TARGET WEBSITE without

understanding its purpose and content." *Id.*

B. Description of Website

The affidavit also described, in great detail, the website whose users were targeted by the investigative technique. It articulated that Website A 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" such as the ones noted in the affidavit. *Id.*, p. 6, ¶ 10. It further articulated that the "administrators and users of the TARGET WEBSITE regularly send and receive illegal child pornography via the website." *Id.* The affidavit also commemorated the massive scale of the site, which appeared to have been operating since August of 2014 – as of February 3, 2015, site statistics indicated that it contained 158,094 members, 9,333 message threads, and 95,148 posted messages.[7]

The affidavit made clear that the illicit purpose was immediately apparent to any user who was able to find the site. As the affiant explained, "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." *Id.*, p. 13, ¶ 12. The following text appeared beneath those prepubescent images: "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 experience, that the phrase "no cross-board reposts" referred to a "prohibition against material that is posted on other websites from being 're-

[7] As the affidavit explained, a bulletin board website such as Website A 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).

posted'" to Website A 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 prepubescent images along with these terms of art referencing image posting and large file compression unmistakably marked Website A as just what it was – a hub for the trafficking of illicit child pornography images and videos on a massive scale.

The affidavit also explained that users were required to register an account by creating a username and password before they could access the site. Users who decided to click 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. That text repeatedly warned prospective users to be vigilant about their security and the potential of being identified, explicitly stating that "the forum operators do NOT want you to enter a real [e-mail] address," that users "should not post information [in their profile] that can be used to identify you," that "it is impossible for the staff or the owners of this forum to confirm the true identity of users," that "[t]his website is not able to see your IP," and that "[f]or your own security when browsing or Tor we also recomend that you turn off javascript and disable sending of the 'referer' header." *Id.*, pp. 14-15, ¶ 13. The repeated security warnings of site administration within those registration terms further marked Website A as a facility of illicit activity.

Once a user accepted those terms and conditions, a user was required to enter a username, password and e-mail account. *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 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. For instance, within the site's "Chan" forum were individual sub-forums for "jailbait"

or "preteen" images of boys and girls. *Id.*, p. 15, ¶ 14. There were separate forums for "jailbait videos" and "Jailbait photos" featuring boys and girls. *Id.* The separate "Pre-teen Videos" and "Pre-teen Photos" forums were each respectively 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."

The affidavit described, in graphic detail, particular child pornography that was posted to and available to all registered users of Website A, that depicted prepubescent females, males and toddlers, being subjected to sexual abuse and exploitation by adults. *Id.*, pp. 17-18, ¶ 18. Although the affidavit clearly stated that "the entirety of [Website A 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 Website A contained a private messaging feature, which allowed users to send messages directly to one another. The affidavit specified that "numerous" site posts referenced private messages related to child pornography, 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 articulated 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 Website A included multiple other features to facilitate the advertisement, distribution and access to 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. The affidavit contained detailed examples and graphic descriptions of prepubescent child pornography disseminated by site users through each one of those features. *Id.*

C. The Network Investigative Technique

The affidavit contained a detailed and specific explanation of the NIT, indicating why its use was necessary, 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 [Website A] would remain unknown" because any IP address logs of user activity on Website A 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 . . . rout[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," whereas the affiant concluded that "using a NIT may help FBI agents locate the administrators and users" of Website A. *Id.*, pp. 23-24, ¶¶ 31-32. The affiant articulated that, 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 Website A 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 Website A 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 computer. *Id.* The exact information to be collected about was detailed in the warrant and accompanying Attachment A, along with technical explanations of the terms. It included the following: (1) an IP address; (2) a unique identifier to distinguish the data from that of other computers; (3) an operating system; (4) information about whether the NIT had already been delivered; (5) a Host Name; (6) an active operating system username; and (7) a 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 the . . . computer and its user." *Id.*, p. 26, ¶ 35. For instance:

> the actual IP address of a computer that accesses [Website A] 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 Website A 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 [Website A]" such as the sub-forums with the most egregious activity which were described elsewhere in the affidavit. Finally, the affidavit re-iterated its specific requests,

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

III. ARGUMENT

The defendant does not challenge the accuracy of any of the information articulated by law enforcement in either of the pertinent warrants. Rather, he unpersuasively argues that the NIT search warrant violated the jurisdictional requirements for searches under Fed. R. Crim. P. 41 and 28 U.S.C. § 636(a). On those purported bases, the defendant contends that evidence seized pursuant to the NIT and the residential warrants should be suppressed. The defendant's arguments are without merit.

A. Summary of Argument

The 31-page NIT search warrant affidavit amply articulated, and the issuing magistrate found, probable cause to deploy the NIT to registered users of a website dedicated to the advertisement and distribution of child pornography which operated on the anonymous Tor network. The warrant particularly described exactly what information would be collected through the NIT – IP address and other computer-related information – and how that information would assist with identifying site users and computers used to access the site. In doing so, the warrant affidavit comprehensively established a fair probability that evidence of a crime – that is, of the identity of perpetrators – would be found via issuance of the warrant.

Moreover, the NIT warrant was issued by a magistrate judge within the jurisdiction of the U.S. District where the website operated during the period of authorization and, accordingly, the District into which registered site users communicated when accessing the website. In any event,

while neither the asserted violation of Rule 41 nor any of the defendant's other arguments warrant suppression, law enforcement acted at all times in good-faith reliance upon warrants issued upon findings of probable cause by three neutral and detached magistrates in two different U.S. Districts. The extreme remedy of suppression is not justified where, as here, law enforcement diligently sought and received judicial authority for investigative techniques that were necessitated by suspects' use of anonymizing technology to criminally exploit children. Accordingly, this court should deny the defendant's motion.

B. The United States Complied With Rule 41 and, In Any Event, Suppression on that Basis is Unwarranted

The NIT search warrant was properly issued by the EDVA magistrate judge. Yet, the defendant argues for suppression based on a purported violation of the geographic limitations of Rule 41. *See* Levin Br. at 6. His argument fails for three separate and independent reasons. First, the First Circuit has rejected suppression as a per se remedy for a Rule 41 violation. Second, the warrant is consistent with Rule 41. Third, courts have common law authority to issue warrants consistent with the Fourth Amendment, and this authority supports the warrant in this case.

At the outset, it is important to make clear the ramifications of the defendant's Rule 41 argument. At the time the government sought the NIT warrant, the defendant and thousands of others were using the Website A to share child pornography. The site was designed to hide the identity and location of its users, so the government had no way to know where the defendant was without first using the NIT authorized by the warrant. Thus, the defendant is not arguing that the government should have sought its warrant elsewhere, or that the government should have more scrupulously followed any of the procedures of Rule 41 for obtaining or executing the warrant. Instead, the defendant is arguing that his use of the Tor hidden service deprived any

court of jurisdiction to issue a warrant to identify him. If the defendant were correct, use of a Tor hidden service could potentially create an insurmountable legal barrier to protecting the children who are harmed by massive criminal enterprises like the targeted hidden service. Fortunately, the defendant is wrong.

First, because violations of Rule 41 are essentially ministerial, "a violation does not require suppression unless the defendant can demonstrate prejudice." *United States v. Burgos-Montes*, 786 F.3d 92, 109 (1st Cir. 2015), citing *United States v. Bonner*, 808 F.2d 864, 869 (1st Cir. 1986). "Prejudice means being subjected to a search that might not have occurred or would not have been so abrasive had the rules been followed." *Burgos-Montes*, 786 F.3d at 109 (internal quotation marks and citations omitted). Although *Burgos-Montes* concerned an alleged violation of Rule 41(e) and *Bonner* involved an alleged violation of Rule 41(d), the First Circuit has noted that "other Circuits have held that the same applies to all prerequisites of Rule 41." *Burgos-Montes*, 786 F.3d at 109. The Seventh Circuit has held that "violations of federal rules do not justify the exclusion of evidence that has been seized on the basis of probable cause, and with advance judicial approval." *United States v. Cazares-Olivas*, 515 F.3d 726, 730 (7th Cir. 2008). In this case, the defendant's argument that the government violated Rule 41 is based on the location of the search, not probable cause or the absence of judicial approval.

The defendant cannot show prejudice, which is required to suppress the warrant in the First Circuit. In this case, the defendant's argument that the government violated Rule 41 is based on the location of the search, not the absence of probable cause or the absence of judicial approval. Where there is probable cause, judicial approval, and the computer server which the defendant accessed to view child pornography was physically located in the jurisdiction where the issuing magistrate was located, there can be no prejudice to the defendant.

In *United States v. Phillip Epich*, a pending child pornography case in the Eastern District of Wisconsin, the District Judge was confronted with the same Rule 41 issue. In *Epich*, the defendant argued that the same NIT warrant at issue in the present case violated Rule 41 because the EDVA magistrate judge, who issued the warrant, had no authority to authorize a search outside of the confines of the EDVA. In accepting in whole the recommended findings of a magistrate judge assigned to preliminarily handle the motion, the District Judge (J. Pepper) explained, "Judge Jones rejected the defendant's argument that, because the Virginia warrant was not limited in geographic scope – in other words, because the NIT could capture data about users who physically might be located all over the map – it violated Federal Rule of Criminal Procedure 41, which sets geographic limits on a magistrate judge's authority to issue a warrant." *United States v. Epich*, 2016 WL 953269 (W.D. Wisc. 2016), at *2. The District Judge (J. Pepper) further noted "[w]hile this court is not bound to accept that recommendation, the court's own review of the pleadings and Judge Jones' decision convince this court that Judge Jones' decision was the correct one." *Id.*

In *United States v. Michaud*, a pending child pornography case in the Western District of Washington, in which the defendant challenged the legality of the same NIT warrant at issue in *Epich* and in the present case, the District Judge denied a motion to suppress based, in part, on an alleged violation of Rule 41. The District Judge (J. Bryan) found that the EDVA "NIT warrant technically violates the letter, but not the spirit, of Rule 41(b)." *United States v. Michaud*, 2016 WL 337263 (W.D. Wash. 2016), at 6. The District Judge went on to note that Rule 41 "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." *Id.* The

District Judge further noted that the argument "that the crimes were committed within the location of Website A, Eastern District of Virginia, rather than on personal computers located in other places under circumstances where users may have deliberately concealed their locations" was a cogent argument, not unreasonable, and did not strain credulity. *Id.*

The District Judge noted that Rule 41(b) violations are "categorized as either fundamental, when of Constitutional magnitude, or technical, when not of constitutional magnitude.... [and] [a]s concluded above, the NIT warrant did not fail for constitutional reasons, but rather was the product of a technical violation of Rule 41(b)." *Id.* The District Judge went on to note that in cases of technical violations, suppression is appropriate where a defendant suffers prejudice or where law enforcement intentionally and deliberately disregarded the rule. *Id.*

In discussing whether Michaud suffered prejudice, the District Judge emphatically rejected the same argument made in the instant case – that but for the NIT warrant the search of the defendant's computer would not have occurred. The District Judge noted that such an argument or interpretation "makes no sense, because under that interpretation, all searches executed on the basis or warrants in violation of Rule 41(b) would result in prejudice, no matter how small or technical the error might be.... [s]uch an interpretation would defeat the need to analyze prejudice separately from the Rule 41(b) violation. *Id.*

The District Judge concluded that Michaud did not suffer prejudice and that he "has no reasonable expectation of privacy of the most significant information gathered by deployment of the NIT, Mr. Michaud's assigned IP address, which ultimately led to Mr. Michaud's geographic location." *Id. at* *7.

Second, the government did not violate Rule 41. Under the best interpretation of that

Rule, Rule 41(b) is flexible enough to allow the issuance of warrants to investigate Tor hidden services.[8] 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." In this case, the warrant authorized the use of a NIT (a set of computer instructions) which was located on a server in the Eastern District of Virginia at the time the warrant was issued. Ex. 1, pp. 22-23, 24 ¶¶ 30, 33; Attachment A. As Rule 41(a)(2)(A) defines "property" to include both "tangible objects" and "information," the NIT constituted property located in the Eastern District of Virginia when the warrant was issued. Moreover, the NIT was deployed only to users of Website A who logged into the website, which was located in EDVA, with a username and password. *Id.*, Att. A. Each of those users – including the defendant – accordingly reached into the jurisdiction of EDVA in order to access the site (and the child pornography images/videos therein). Thus, Rule 41(b)(2) provided sufficient authority to issue the warrant for use of the NIT outside of the Eastern District of Virginia.

Similarly, 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

[8] 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 proposed rule was approved by the Advisory Committee on the Criminal Rules in March 2015 and the Standing Committee in May 2015. It is now pending further review before the U.S. Judicial Conference. *See* http://www.uscourts.gov/rules-policies/pending-rules-amendments.

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 in the Internet context. Investigators installed the NIT in the Eastern District of Virginia on the server that contained the targeted child pornography hidden service. When the defendant logged on and retrieved information from that server, he also retrieved the NIT. The NIT then sent network information to law enforcement. Although this network information was not itself location information, investigators subsequently used this network information to identify and locate the defendant. Thus, if Rule 41(b)(2) did not provide authority to issue the warrant, Rule 41(b)(4) did so.

Furthermore, the Virginia warrant was issued by a judge in the district with the strongest known connection to the search: the defendant retrieved the NIT from a server in the Eastern District of Virginia, 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." In addition, the defendant's use of the Tor hidden service made it impossible for investigators to know what other districts, if any, the execution of the warrant would take place in. 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 Virginia 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. U.S.*, 441 U.S. 238, 258 (1979). For these reasons, this Court should conclude that issuance of the warrant did not violate Rule 41.

Third and finally, even if this warrant was not authorized by Rule 41, it was still properly issued by the EDVA magistrate judge. Courts have inherent power to issue search warrants

consistent with the Fourth Amendment. *See United States v. Villegas*, 899 F.2d 1324 (2nd Cir. 1990) (upholding warrant for search of property without seizure and stating: "Rule 41 does not define the extent of the court's power to issue a search warrant. . . . Given the Fourth Amendment's warrant requirements, and assuming no statutory prohibition, the courts must be deemed to have inherent power to issue a warrant when the requirements of that Amendment are met."). Because the warrant was consistent with the Fourth Amendment, it was properly issued.

The defendant also cites 28 U.S.C. § 636(a) as a separate ground in support of his motion to suppress. The defendant spends little or no time distinguishing Rule 41 from 28 U.S.C. § 636(b) and argues that both provisions limit magistrate judges to issuing warrants only in the jurisdiction where they have been appointed. As the defendant uses the two provisions interchangeably, there is no need to further expound on 28 U.S.C. § 636(b). The same rationale for allowing the NIT warrant in this case under Rule 41 also applies to allowing it under 28 U.S.C. § 636(b).

C. The Good-Faith Exception Applies to Evidence Seized Pursuant to All Warrants in this Case

Even if the Court were to find that the NIT affidavit is deficient, the evidence seized pursuant to that search warrant and the subsequent residential warrant, is still admissible under the good-faith exception to the exclusionary rule. In *United States v. Leon*, 468 U.S. 897 (1984), the Supreme Court held that in the absence of an allegation that the magistrate abandoned his detached and neutral role, suppression is appropriate only if the officers were dishonest or reckless in preparing their affidavit or could not have harbored an objectively reasonable belief in the existence of probable cause. *Id.* at 926. Such determinations must be made on a case-by-case basis with suppression ordered "only in those unusual cases in which exclusion will further the purpose of the exclusionary rule." *Id.* at 918.

The exclusionary rule is intended to deter police misconduct, but not to punish errors of judges and magistrates. *Massachusetts v. Shepard*, 468 U.S. 981, 988-90 (1984). There was no police misconduct in this case. The law enforcement officers executing both the NIT warrant and the residential warrant acted in good faith and with reasonable reliance on warrants issued by federal magistrates.

The Defendant does not contend, nor does he cite to any evidence, that either of the separate magistrate judges who approved the warrants pertinent to this case abandoned their neutral and detached role. The defendant also makes no allegation that any of the information articulated any of the three warrants was dishonest or reckless. Further, as noted herein, the comprehensive 31-page NIT affidavit amply articulated probable cause for the requested technique. The defendant alleges without justification that "the officers acted in intentional and deliberate disregard of Rule 41." Defendant's Motion to Suppress at p. 17. This is not accurate. Law enforcement officers relied upon that warrant, its fruits, and the subsequent warrant authorizing searches of the defendant's residence in order to seize relevant evidence in this case. Accordingly, the court should find that all of the evidence the defendant requests the court to suppress is admissible pursuant to the good-faith exception.

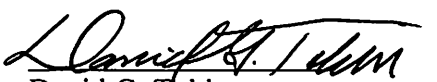
The defendant contends that a proposed amendment to Rule 41 to clarify that courts have venue to issue a warrant "to use remote access to search electronic storage media" inside or outside an issuing district if "the district where the media or information is located has been concealed through technological means" indicates that the NIT warrant was impermissible. The defendant essentially argues that the existence of the proposed amendment supports a finding that the "officers acted in intentional and deliberate disregard of Rule 41" and the good faith

exception should not apply. That argument is mistaken. At the time the Department of Justice proposed the Rule 41 Amendment, a single magistrate judge had rejected a warrant to locate a computer concealed through technological means, see *In re Warrant*, 958 F. Supp. 2d 753 (S.D. Tex. 2013), but every other magistrate judge known to consider the issue had issued such a warrant. See, e.g., *United States v. Cottom, et. al.*, No. 13-cr-108 (D. Neb. Oct. 14, 2014) (Doc #122, Attachment 1) (search warrant); *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", No. 07-mj-5114* (W.D. Wash. June 12, 2007), available at http://www.politechbot.com/docs/fbi.cipav.sanders.affidavit.071607.pdf (search warrant). Under these circumstances, the proposed amendment is properly understood as clarifying existing authority, not creating new authority. Nor is such a clarification unusual. As the government argued previously, the NIT warrant complied with the existing Rule 41.

IV. CONCLUSION

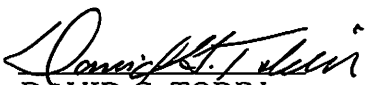
The United States of America respectfully requests that this Court deny the defendant's motions to suppress evidence for the above stated reasons.

CARMEN M. ORTIZ
United States Attorney

By: 
David G. Tobin
Jordi de Llano
Assistant United States Attorneys

CERTIFICATE OF SERVICE

I hereby certify that this document which is filed under seal was delivered by email to the attorney of record for the defendant on March 18, 2016.

By: 
DAVID G. TOBIN
Assistant U.S. Attorney

Date: March 21, 2016