STEVEN G. KALAR
Federal Public Defender
HANNI M. FAKHOURY
Assistant Federal Public Defender
1301 Clay Street, Suite 1350N
Oakland, CA 94612
(510) 637-3500
hanni_fakhoury@fd.org

Attorneys for DUMAKA HAMMOND

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. DUMAKA HAMMOND, Defendant.	CR 16-102-JD MOTION TO SUPPRESS NIT SEARCH WARRANT Hearing Date: July 21, 2016 Time: 9:30 a.m.

TO: BRIAN STRETCH, UNITED STATES ATTORNEY; AND
THOMAS R. GREEN, ASSISTANT UNITED STATES ATTORNEY:

PLEASE TAKE NOTICE that the defendant DUAMAKA HAMMOND hereby moves this Court for an order suppressing the Network Investigative Technique search warrant issued in of the Eastern District of Virginia. This motion will be heard on July 21, 2016 at 9:30 a.m. in Courtroom 2, on the Fourth Floor of the Oakland Courthouse.

This motion is based on this notice and motion, the attached memorandum of points and authorities and accompanying exhibits, the United States Constitution, Federal Rule of Criminal Procedure 41, all other applicable constitutional, statutory and case authority and such evidence and argument that may be presented at the motion hearing.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

INTRODUCTION

Between February 20 and March 4, 2015, the FBI operated a child pornography website, disseminating thousands of images of child pornography across the Internet, and the world. As Massachusetts District Judge William G. Young recently wrote, "the government disseminated the child obscenity to catch the purchasers—something akin to the government itself selling drugs to make the sting." *United States v. Levin*, ___ F.Supp.3d ___, 2016 WL 2596010, *8 n. 12 (D. Mass. May 5, 2016). In order to "make the sting," the FBI used a Network Investigative Technique ("NIT"), a piece of computer code that the FBI deployed onto the computers of users who accessed a website that contained child pornography. The NIT obtained identifying information about visitors to the site, including the IP addresses of computers visiting the site. The FBI then used administrative subpoenas to identify the physical locations associated with those IP addresses, and ultimately obtained individualized search warrants for the residences associated with the IP address.

The deployment of the NIT was authorized by a single magistrate judge in the Eastern District of Virginia ("EDVA"). Although Federal Rule of Criminal Procedure 41 and the Federal Magistrates Act, 28 U.S.C. § 636, limits a magistrate judge's ability to authorize a search to the district where the magistrate judge sits except in certain narrow situations, the NIT warrant reached far beyond the Eastern District of Virginia. There are currently federal criminal cases charged as a result of the NIT in Massachusetts, New York, Ohio, Oklahoma, Pennsylvania, Texas, Washington, West Virginia, Wisconsin and, now in Mr. Hammond's case, the Northern District of California.

Four different district court judges (and one magistrate judge) have found the same exact NIT search warrant involved in Mr. Hammond's case violated the territorial—and jurisdictional—limitations in Federal Rule of Criminal Procedure 41 and two have suppressed the NIT search warrant, and all the fruits obtained as a result of the NIT search warrant. Mr. Hammond requests this Court follow these decisions, find the NIT search warrant violated Federal Rule of Criminal Procedure 41 and suppress the NIT search warrant and the fruits of that search.

STATEMENT OF FACTS

The facts pertinent to this motion to suppress are largely not in dispute and the other cases stemming from this investigation involve essentially the same set of facts.

A. The FBI's Investigation and Seizure of the PlayPen Child Pornography Website.

Beginning in September 2014, FBI agents began investigating a child pornography website variably identified as TARGET WEBSITE or WEBSITE A in search warrant affidavits, which has now been publicly identified as "PlayPen." The site was accessed on the Tor computer network.

The Tor network consists of a computer network and software that provide Internet users with online anonymity. Tor was initially developed by the United States Naval Research Lab in the 1990s and is now run as an independent non-profit organization. Tor works by obscuring how and where users access the Internet. Users first download Tor software onto their computers. The software allows users to connect to the Tor network, which is a network of computers—known as "nodes" or "relays"—operated by volunteers. When a user connects to the Tor network, their Internet traffic does not go directly to the website they are seeking. Instead, a Tor user's Internet traffic connects to a volunteer node or relay, which passes the user's Internet traffic on to another volunteer node or relay, and then to another node or relay (and perhaps many other nodes or relays) until it exits through an "exit node" and connects to the site. This allows users to mask their true location when they visit a site. Specifically, the site will only know the IP address of exit node computer, and not the original computer that sought to access the site.[1]

Tor also provides users with other services, including an anonymous web hosting service known as a "hidden service." A Tor hidden service is a website hosted on the Tor network which does not reveal its location. For example, rather than displaying a URL like www.cand.uscourts.gov, the site's location would be replaced with a Tor based web address such as dboevtdpvsuthpw.onion. Tor hidden service websites always end in .onion and can only be accessed through the Tor network. As a result, a Tor user can connect to a Tor hidden service site without knowing the site's location and without the site knowing the visitor's location.[2]

[1] *See generally* https://www.torproject.org/about/overview.html.en.

[2] *See generally* https://www.torproject.org/docs/hidden-services.html.en.

PlayPen operated as a Tor hidden service that could only be accessed through the Tor network. In order to access the site, a visitor was required to login with a username and password. *See* Exhibit A, Eastern District of Virginia Search Warrant 15-SW-89 ("NIT Warrant") at ¶ 12. Once logged in, a visitor could view the content on the site, which included discussion forums, private messaging services, and images of child pornography. *Id.* at ¶¶ 12-14.

In December 2014, a foreign law enforcement agency informed the FBI that it had a suspected United States based IP address for the site. *Id.* at ¶ 28. The FBI investigated the IP address and determined that the website was hosted on a server in Lenoir, North Carolina. *Id.* In January 2015, the FBI obtained and executed a search warrant in the Western District of North Carolina, and seized the server that hosted the Playpen website. *Id.* Rather than shut down the website, however, the FBI placed a copy of the seized server, including the child pornography contained on the Playpen site, onto a government controlled server in Newington, Virginia. *Id.*

B. <u>The FBI Operates the PlayPen Child Pornography Site In Order to Deploy an NIT.</u>

On February 20, 2015, prosecutors in the Eastern District of Virginia submitted an application and affidavit for a search warrant to U.S. Magistrate Judge Theresa Carroll Buchanan in Alexandria, Virginia. In the affidavit, the government explained that it wanted to continue operating the Playpen site from a "government-controlled computer server in Newington, Virginia, on which a copy of TARGET WEBSITE currently resides." Exh. A at ¶ 30. It explained it wanted to operate the site for 30 days in order to locate and identify visitors to the site. *Id.* at ¶ 29-30. The warrant affidavit explained that in order to identify the users of Playpen, it would need to deploy an additional investigative tool to work around the fact that the Tor network was obfuscating the visitor's IP address. The government thus requested authorization to deploy a Network Investigative Technique ("NIT") which it believed had a "reasonable likelihood" to locate administrators and users of the site. *Id.* at ¶ 31; *see also id.* at ¶¶ 32-37.

The NIT was simply computer software that the government inserted into the PlayPen site. According to the search warrant affidavit, the government would deploy the NIT—that is, send it to the user's computer—anytime a visitor to Playpen entered a username and password to access the site. Once a visitor to the site entered their username and password, the FBI controlled server would use the NIT to force the user's computer to collect information directly from the user's computer and then transmit that information back to the FBI. *Id.* at ¶ 36. The specific information collected by the NIT were:

- The "activating" computer's actual IP address and the date and time the NIT determined what that IP address was;
- A unique identifier generated by the NIT to distinguish the different data obtained from other "activating" computers;
- The type of operating system running on the "activating" computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86);
- Information about whether the NIT has already been delivered to the "activating" computer;
- The "activating" computer's "host name," which is the name assigned to a device connected to a computer network used to identify the specific device;
- The "activating" computer's active operating system username; and
- The "activating" computer's Media Access Control ("MAC") address, which is a unique identifying number associated with computers.

Id. at ¶ 34. The NIT application noted the FBI may target particular users and administrators "more discreetly," but ultimately sought authorization to deploy the NIT to investigate "any user" who logged into the site with a username and password, regardless of their physical location, whether or not they were using the site's chat features, or viewing child pornography. *Id.* at ¶ 33 fn. 8.

The magistrate judge signed the warrant that same day and authorized the government to deploy the NIT for 30 days. The Court also granted the government's request to delay notice of the search until 30 days "after any individual assessing the TARGET WEBSITE has been identified to a sufficient degree as to provide notice" under 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3). *Id.* at ¶ 40.

On the same day the government applied for the NIT warrant, EDVA prosecutors also applied for an order under the Wiretap Act, 18 U.S.C. §§ 2510, et seq., to authorize the interception of communications taking place on Playpen. *See* Exhibit B, Eastern District of Virginia Wiretap Order

15-ES-4 ("Wiretap Order"). The wiretap affidavit noted the site had a "chat" feature and allowed users to send private messages to each other. The government thus requested the ability to intercept communications on the site in real time. The application and affidavit submitted in support of the wiretap explained that the "TARGET WEBSITE will continue to operate from the government-controlled computer server in Newington, Virginia, on which a copy of TARGET WEBSITE currently resides." *Id.* at ¶ 52. The wiretap affidavit also explained the NIT and noted that the "deployment of a NIT to attempt to identify actual IP addresses" and the interception of electronic communications on the site are "the only available investigative technique with a reasonable likelihood of securing the evidence necessary to prove beyond a reasonable doubt the identity of the TARGET SBUJECTS." *Id.* at ¶ 58. U.S. District Judge Anthony J. Trenga signed the wiretap order that same day.

Equipped with the NIT warrant and wiretap order, the government began deploying the NIT on February 20, 2015. Although the government was authorized to deploy the NIT for 30 days, on March 4, 2015, it abruptly stopped deploying the NIT and took the Playpen website offline. Now armed with IP addresses (and more) of users accessing the Playpen site, the government began making individualized cases in federal courts across the country. The press has reported at least 135 federal cases have been filed in 18 different states across the country.[3]

C. <u>The Search Warrant for 678 8th Street, Richmond, California.</u>

On July 16, 2015, FBI Special Agent Robert Basanez submitted a search warrant application for 678 8th Street in Richmond, California to the Honorable Magistrate Judge Maria-Elena James in San Francisco. *See* Exhibit C, Northern District of California Search Warrant 15-70905 ("Richmond Warrant"). The search warrant was related to an investigation into the possession and access with intent to view child pornography in violation of 18 U.S.C. § 2252A. Exh. C at ¶ 2. It specifically claimed that an Internet account located at the Richmond address "has been linked to an online community of individuals who regularly send and receive child pornography via a website that

[3] *See* Gabrielle Banks, "Federal agents sweep child pornography site by hacking 'dark web' site," *Houston Chronicle*, April 10, 2016, *available at* http://www.houstonchronicle.com/news/houston-texas/houston/article/Federal-agents-sweep-child-pornography-site-by-7240097.php.

operated on an anonymous online network." *Id.* at ¶ 6.

Agent Basanez's affidavit explained in detail the PlayPen site and the NIT search warrant previously issued in the Eastern District of Virginia. *Id.* at ¶¶ 7-24. It noted that "Website A" had been seized in Lenoir, North Carolina on February 20, 2015 and from that date until March 4, 2015, the site was operating in Newington, Virginia. *Id.* at ¶ 11. Agent Basanez's affidavit explained that between February 20, 205 and March 4, 2015, the government "monitored electronic communications of users of 'Website A'" and had examined and documented the contents of the site. *Id.* The affidavit explained the Eastern District of Virginia search warrant that authorized the government to deploy the NIT, and explained the information that the NIT captured. *Id.* at ¶ 24.

Unlike the wiretap order or the NIT search warrant, the affidavit submitted by Agent Basanez to Judge James was conspicuously silent about the fact that the PlayPen site was operating on a *government controlled* server in Newington and that it was the FBI itself that was operating the website. *Compare with* Exh. A at ¶ 30 ("The TARGET WEBSITE will continue to operate from the government-controlled computer server in Newington, Virginia"); Exh. B at ¶ 52 (same). The Richmond search warrant simply noted that after PlayPen was seized in Lenoir, North Carolina, the "website operated in Newington, Virginia, from February 20, 2015, until March 4, 2015, at which time 'Website A' ceased to operate." Exh. C at ¶ 11.

With respect to the specific search warrant request for the house in Richmond, Agent Basanez's affidavit explained that the NIT determined that one of Playpen's users went by the name "jerkjerk." Exh. C at ¶ 25. The NIT also determined that the computer host name for the user "jerkjerk" was "JohnRR-PC" and the computer login was "Maka." *Id.* at ¶ 34. Most importantly, the NIT determined the IP address "jerkjerk" was using to connect to Playpen. *Id.* at ¶ 32. The FBI used an administrative subpoena to determine that the IP address was assigned by Comcast to 678 7th Street in Richmond, California and that the account was in Mr. Hammond's name. *Id.* at ¶ 33. Once Mr. Hammond had been identified by the NIT and the administrative subpoena to Comcast, the government did cursory surveillance and looked Mr. Hammond up in public databases. *See id.* at ¶¶ 36-41. Judge James signed the warrant on July 16, 2015.

But for the results of the NIT search warrant, the FBI would not have had probable cause to obtain a search warrant for the house in Richmond.

D. Execution of the Richmond Search Warrant and Mr. Hammond's Arrest.

The following day, July 17, 2015, the FBI executed the search warrant on the Richmond residence. *See* Exhibit D, July 28, 2015 FBI Form 302 Report of Investigation. According to the FBI's report of the search, when the agents entered the house, they saw Mr. Hammond walking with a laptop in his hand.[4] They seized the laptop in Mr. Hammond's hand, as well as two other laptop computers and an external hard drive from the residence. *Id.* According to the discovery provided by the government, the agents questioned Mr. Hammond but did not arrest him.

On March 10, 2016, a one count indictment was filed charging Mr. Hammond with possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). An arrest warrant was issued in connection with the indictment. That same day, FBI Special Agent Basanez arrested Mr. Hammond in San Francisco, as Mr. Hammond was leaving work. At the time of Mr. Hammond's arrest, the government seized a number of items from Mr. Hammond, including his cell phone and a laptop computer. According to the discovery produced by the government, hash values of child pornography images located on PlayPen were allegedly found on one of the laptops seized from the Richmond house.

ARGUMENT

The magistrate judge in the Eastern District of Virginia had no authority under the Federal Magistrates Act, 28 U.S.C. § 636, or Federal Rule of Criminal Procedure 41 to authorize a search outside the boundaries of the Eastern District of Virginia. But the NIT warrant did precisely that, deploying a surveillance tool via a broad dragnet that touched computers across the United States, including here in the Northern District of California, and abroad.[5] At least four different district courts (and one magistrate judge) reviewing the NIT warrant have concluded the warrant was not

[4] For purposes of this motion, Mr. Hammond assumes all the facts contained in the FBI's Report of Investigation are true. However, he reserves the right to dispute any facts in the report in future court proceedings.

[5] *See* Joseph Cox, "The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers," *Motherboard*, January 5, 2016, *available at* https://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers.

authorized under Rule 41. *See United States v. Werdene*, ___ F.Supp.3d ___, 2016 WL 3002376 (E.D. Pa. May 18, 2016); *Levin*, 2016 WL 2596010, *5-6; *United States v. Michaud*, 2016 WL 337263, *5-6 (W.D. Wash. Jan. 28, 2016); *see also* Exh. E, *United States v. Arterbury*, 15-cr-182-JHP (N.D. Okla. Apr. 25, 2016) (report and recommendation of magistrate judge, adopted by the district court May 12, 2016). Two courts have suppressed the fruits of the NIT warrant as a result. *Levin*, 2016 WL 2596010, *5-6; Exh. E, *Arterbury*, at p. 27.

Mr. Hammond asks this Court to do the same, find the NIT warrant violated Rule 41 and the Federal Magistrates Act and suppress the NIT warrant and its fruits, specifically (1) the search warrant for the Richmond house; (2) all evidence seized and searched as a result of the Richmond search warrant; (3) any statements made by Mr. Hammond to the FBI in July 2015 when the Richmond search warrant was being executed; and (4) any evidence obtained from or statements made by Mr. Hammond as a result of his arrest in March 2016.

A. **The NIT Warrant Was Not Authorized Under Rule 41(b).**

A magistrate judge's jurisdiction—and authority—is limited by Congressional statute. *United States v. Colacurcio*, 84 F.3d 326, 328 (9th Cir. 1996). Under the Magistrates Act, 28 U.S.C. § 636, Congress has authorized magistrate judges "within the district in which sessions are held by the court that appointed the magistrate judge" to exercise all the power authorized by the Federal Rules of Criminal Procedure. 28 U.S.C. § 636(a)(1). In other words, a magistrate judge's authority to authorize a search warrant comes from Federal Rule of Criminal Procedure 41 and no other source. *See Levin*, 2016 WL 2596010, at *4.

Rule 41 in turn permits a magistrate judge to authorize a search in five circumstances:

- When the person or property to be searched or seized is "located within the district;"
- When the person or property to be searched or seized is outside the district if the person or property is within the district when the warrant is issued but may move outside the district before the warrant is executed;
- When the person or property to be searched or seized is connected to a terrorism investigation where activities occurred within the district regardless of whether the person or property is within the district or not;

- To install a "tracking device" within the district to track the movement of a person or property regardless of whether they are in the district or not; and
- On some federal property or diplomatic or consular missions, regardless of where it is located, when criminal activity occurred within the district of the issuing magistrate judge.

Fed. R. Crim. P. 41(b). In other NIT cases, the government has claimed that the NIT warrant falls under three of these subsections: (1) the property to be searched was within the Eastern District of Virginia; (2) the property to be searched is within the Eastern District of Virginia but may move outside the district; and (3) the NIT is a "tracking device" that was installed in the Eastern District of Virginia. *See Levin*, 2016 WL 2596010, at *5. But it is clear the NIT warrant is not authorized under Rule 41(b) at all.

1. The NIT Warrant was not Authorized by Rule 41(b)(1) or (b)(2) Because the "Activating Computers" Searched by the NIT Were Not Located in the EDVA.

First, the property to be searched is clearly not located in the Eastern District of Virginia. The NIT warrant stated the evidence sought is "located in the Eastern District of Virginia," but that is not true. *See* Exh. A. Only the PlayPen site—under the FBI's control—was located in the Eastern District of Virginia on a FBI controlled server in Newington. The actual place to be searched were the "activating computers—wherever located" that would ultimately be infected with the NIT. *Id.* at ¶ 46. The assertion that computers would be searched "wherever located" indicated that the government simply had no idea where the computers that would receive the NIT would be located. *Id.* at ¶ 46(a). Ultimately, the objective of the NIT was *not* to obtain information from the FBI's server in the Eastern District of Virginia. *See id.* at ¶ 32. Instead, the Wiretap application explained the NIT was needed because possession of the server alone did not allow the government to identity PlayPen's users. Exh. B at ¶ 58. Only by deploying the NIT onto individual computers would the government be able to obtain the IP addresses, MAC addresses, and other identifying information about specific computers in order to locate and identify PlayPen users. *Id.* Judge Young of the District of Massachusetts has rejected the argument that the search took place in the Eastern District of Virginia as "a strained, after-the-fact rationalization." *Levin*, 2016 WL 2596010, at * 5; *see also*

Michaud, 2016 WL 337263, at *6 ("the object of the search and seizure was Mr. Michaud's computer"). Thus, the search was not authorized under Rule 41(b)(1).

Because the computers to be searched by the NIT warrant were not located in the Eastern District of Virginia, the search also fails to satisfy Rule 41(b)(2) which authorizes a search for property that was in the district but moved out of the district before the search could take place. As explained above, the place the NIT searched was the computer located outside of the Eastern District of Virginia, not the server that hosted PlayPen. The computers seized from Mr. Hammond in Richmond, California were never alleged to be in the Eastern District of Virginia; and even if the Court believes Mr. Hammond's computers interacted with a computer in the Eastern District of Virginia, that was only *after* the warrant was executed and the NIT was deployed onto his computer here in the Northern District of California. *See* Exh. E, *Arterbury* at p. 16.

2. The NIT Warrant Was Not Authorized By Rule 41(b)(4) Because the NIT is not a "Tracking Device" and the Installation of the NIT Did Not Occur in the EDVA.

Finally, numerous courts have rejected the argument that the NIT was the equivalent of a "tracking device" under Rule 41(b)(4). Most critically, the installation of the NIT did not take place in the Eastern District of Virginia but in the district where the computer was physically located. *See Levin*, 2016 WL 2596010, at * 6, n. 9; *Michaud*, 2016 WL 337263, at *6; *see also In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.Supp.2d 753, 758 (S.D. Tex. 2013) (rejecting government's application for a warrant to deploy software to remotely extract identifying information from a computer in an unknown location, because "there is no showing that the installation of the 'tracking device' (*i.e.* the software) would take place within this district. To the contrary, the software would be installed on a computer whose location could be anywhere on the planet.").

Thus, the NIT warrant did not fall within any of the provisions of Rule 41. The result is "because the magistrate judge lacked authority, and thus jurisdiction, to issue the NIT Warrant, there simply was no judicial approval" and the NIT warrant is *void ab initio*. *Levin*, 2016 WL 2596010, at *8; *see also United States v. Master*, 614 F.3d 236, 239 (6th Cir. 2010) ("when a warrant is signed by someone who lacks the legal authority necessary to issue search warrants, the warrant is *void ab* *initio.*”).

B. Suppression is the Appropriate Remedy for the Rule 41 Violation.

When a search occurs in violation of Rule 41, suppression is appropriate if (1) the violation rises to a “constitutional magnitude,” (2) the defendant was prejudiced because the search would not have occurred if the rule had been followed; or (3) law enforcement acted in “intentional and deliberate disregard” of Rule 41. *United States v. Weiland*, 420 F.3d 1062, 1071 (9th Cir. 2005) (quotations and citations omitted). The Court need not find all three are present; just one is sufficient to require suppression. Here, however, all three are met and suppression is warranted for each of these reasons.

1. The Rule 41 Violation is Constitutional, Not Merely Technical.

The violation here is not a “technical” violation of Rule 41, but one that speaks to the substantive constitutional protections embodied in Rule 41. *See United States v. Williamson*, 439 F.3d 1125, 1133 (9th Cir. 2006) (distinguishing between Rule 41 violations that are “mere technical error” and those rising to a “constitutional magnitude.”). The Seventh Circuit has explained that “Rule 41(b) deals with substantive judicial authority—not procedure.” *United States v. Berkos*, 543 F.3d 392, 398 (7th Cir. 2008).

In *Levin*, the District of Massachusetts found the Rule 41 violation triggered the substantive protections of the rule because the error involved “the authority of the magistrate judge to issue the warrant” rather than simply “the procedures for obtaining and issuing warrants.” *Levin*, 2016 WL 2596010, at *7-8 (quoting *United States v. Krueger*, 809 F.3d 1109, 1115 n. 7 (10th Cir. 2015) (quotations omitted)). More specifically, the court found that since “the magistrate judge lacked authority, and thus jurisdiction, to issue the NIT Warrant, there simply was no judicial approval.” *Levin*, 2016 WL 2596010, at *8. Without jurisdiction to issue the warrant, it was simply “void.” *Id.*

Other courts have reached similar results with respect to warrants that violated the jurisdictional limitations of Rule 41. In *United States v. Glover*, 736 F.3d 509 (D.C. Cir. 2013), the D.C. Circuit suppressed a Title III wiretap order that was issued in the District of D.C. but authorized the interception of communications in the District of Maryland and the Eastern District of Virginia. 736 F.3d at 510. The D.C. Circuit concluded that the wiretap violated both Title III and Rule 41(b), which it found "impose the same geographic limitations on warrants." *Id.* at 515. The warrant's failure to comply with Rule 41(b)'s geographic limitations was a "jurisdictional flaw" that could not be excused as a "technical defect" because the error was a "blatant disregard of a district judge's jurisdictional limitation." *Id.*

The problems with the NIT warrant rise to constitutional error. Since the NIT warrant was not authorized by Rule 41, it was *void ab initio*. A search conducted under a facially deficient warrant is considered warrantless. *See Groh v. Ramirez*, 540 U.S. 551, 558 (2004) (finding "warrant was so obviously deficient that we must regard the search as 'warrantless'"). The "most basic" Fourth Amendment rule is that warrantless searches "are per se unreasonable under the Fourth Amendment." *Coolidge v. New Hampshire*, 403 U.S. 443, 454-55 (1971). The Fourth Amendment prohibits searches "conducted pursuant to an ill-begotten or otherwise invalid warrant." *Bravo v. City of Santa Maria*, 665 F.3d 1076, 1083 (9th Cir. 2011). Because the magistrate judge had no jurisdiction to authorize the NIT search warrant, it was invalid and deficient. Since that error resulted in a warrantless search of Mr. Hammond's residence and computer, suppression is appropriate.[6]

2. Mr. Hammond Was Prejudiced Because the July 2015 and March 2016 Searches of Mr. Hammond and His Computers, as well as His Statements to the FBI During the Search of His Residence, Would Not Have Occurred if Rule 41(b) Had Been Followed.

A defendant is prejudiced by a Rule 41 violation if the search of his property would not have occurred but for the Rule 41 violation. *Weiland*, 420 F.3d at 1071. Two other courts considering this same exact NIT warrant have found that defendants were prejudiced by the Rule 41 violation and suppressed the NIT warrant and subsequent search warrants obtained as a result of the NIT warrant.

In *Levin*, the District of Massachusetts found prejudice, finding that "the government might not have obtained the evidence it seized pursuant to the Residential Warrant, since the application for that warrant was based on information it acquired through the execution of the NIT Warrant."

[6] Mr. Hammond anticipates filing a subsequent motion to suppress the NIT search warrant for violating the Fourth Amendment, and so this motion does not include a full Fourth Amendment analysis of the NIT warrant.

Levin, 2016 WL 2596010, at *9 n. 16. The court noted "the government itself points out, it 'had no way to know where the defendant was without first using the NIT.'" *Id.* (quoting Government's response brief). It rejected the government's argument that there was no prejudice because there was probable cause of criminal activity, noting "this is not the standard for determining prejudice." *Id.* at *9; *see also Coolidge*, 403 U.S. at 451 (warrantless search "unlawful notwithstanding facts unquestionably showing probable cause.") (quotation and citation omitted).

Similarly, in *Arterbury*, the Northern District of Oklahoma found prejudice because the defendant's computers would not have been searched had Rule 41(b) been followed since absent the government's deployment of the NIT, the physical location—IP address—of the computers accessing PlayPen would not have been known. Exh. E, *Arterbury*, at 22. *Arterbury* relied on the Tenth Circuit's decision in *United States v. Krueger*, 809 F.3d 1109 (10th Cir. 2015), which involved a computer believed to contain child pornography that was seized in the Western District of Oklahoma pursuant to a search warrant authorized by a magistrate judge in the District of Kansas. 809 F.3d at 1111-12. The Tenth Circuit found that the Rule 41 violation prejudiced the defendant because but for the improper search warrant, the search ultimately would not have occurred. *Krueger* rejected the argument that "the Government *may have* been able to obtain a warrant from a federal magistrate judge" in the correct district, noting "such hypotheticals simply cannot cure the Government's gross negligence in failing to comply with Rule 41(b)(1) in the first instance." *Id.* at 1117 (citing *Glover*, 736 F.3d at 514-15) (emphasis in original).

Here, there is no question that but for the Rule 41 violation, Mr. Hammond's residence and computer would not have been searched. Had Rule 41 been followed, the NIT Warrant would have only authorized the deployment of the NIT on "activating computers" located within the Eastern District of Virginia. Obviously, Mr. Hammond's residence and computer were not located in that district. Moreover, but for the NIT warrant, the subsequent Richmond search warrant signed in this district by Judge James would not have issued. The entire basis of the Richmond search warrant was the evidence obtained from the NIT search warrant. *See* Exh. C at ¶¶ 7-41.[7] It was the NIT that

[7] The search warrant submitted to Judge James did reference additional facts about Mr. Hammond, including his prior convictions for possession of child pornography, his status as a registered sex

allowed the government to discover the IP address that the FBI investigated and tracked down to Mr. Hammond's residence in Richmond. *Id.* at ¶¶ 27, 32-33. And as a result of the Richmond search warrant, the government obtained statements from Mr. Hammond, seized computers and property belonging to Mr. Hammond, and secured the present indictment and an additional search of Mr. Hammond and his property upon his arrest.

The district court in *Michaud* analyzed this same exact NIT warrant, found a Rule 41 violation but determined there was no prejudice, believing since individuals have no Fourth Amendment expectation of privacy in their IP address, the government "eventually could have [] discovered" that information. *Michaud*, 2016 WL 337263, *7. But that is wrong for two reasons.

First, to the extent the Ninth Circuit has found no expectation of privacy in an IP address, that was only with respect to an IP address the government attempted to obtain from a *third party service provider*, not information obtained from communicating with a user's computer directly. *See, e.g., United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2007) (finding no expectation of privacy when government installed pen register on Internet service provider's equipment at their facility).[8] Here, the NIT obtained the IP address from the "activating computers" directly and not by going to a third party service provider and seeking IP address information from the service provider's own facilities or records. There is no question that there is an expectation of privacy on the information stored on and generated by a person's computer and as a result, the Fourth Amendment applies. *See United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008) ("as a general

offender, and a police report filed against him in February 2014. *See* Exh. C at ¶¶ 41-45. But those details were irrelevant without the NIT's determination that an IP address associated with Mr. Hammond's residence accessed child pornography. In other words, the only way for the FBI to learn those facts about Mr. Hammond was because the NIT had identified the IP address of Mr. Hammond's residence as a visitor to PlayPen in the first place. Without the IP address, obtained via the NIT, those facts alone would not have provided probable cause to issue a search warrant for Mr. Hammond's residence.

[8] Several judges in the Northern District of California, in the context of historical cell site location information, have rejected the argument that an individual has no Fourth Amendment expectation of privacy in third party digital information that reveals a person's location. *See, e.g., United States v. Williams*, ___ F. Supp.3d ___, 2016 WL 492933, *3 (N.D. Cal. Feb. 9, 2016) (Orrick, D.J.); *In re Telephone Information Needed for a Criminal Investigation*, 119 F. Supp.3d 1011, 1020-26 (N.D. Cal. 2015) (Koh, D.J.); *United States v. Cooper*, 2015 WL 881578, *6-8 (N.D. Cal. Mar. 2, 2015) (Illston, S.D.J.).

matter an individual has an objectively reasonable expectation of privacy in his personal computer").

In *Riley v. California*, 134 S. Ct. 2473 (2014) the Supreme Court rejected the exact argument that the district court in *Michaud* relied upon. In *Riley*, the Court ruled that the Fourth Amendment's search incident to arrest exception to the Fourth Amendment warrant requirement did not extend to a cell phone found on an arrestee's person at the time of their arrest. Before the Supreme Court, the government argued that police should be permitted to search incident to arrest a cell phone's call log consistent with *Smith v. Maryland*, 442 U.S. 735 (1979) which found no expectation of privacy in a person's dialing records. *Riley,* 134 S. Ct. at 2492. But the Supreme Court unanimously rejected that faulty analogy, noting that *Smith* only authorized the installation of a pen register on the phone company's equipment since that was not a "search" under the Fourth Amendment. Obtaining the same information from the phone directly—as opposed to obtaining it from the phone company—was indisputably a "search" protected by the Fourth Amendment. *Riley*, 134 S. Ct. at 2492-93.

Second, contrary to the district court's belief in *Michaud*, the IP address information was not available from other sources. According to the affidavit the government submitted in support of its request for a Title III wiretap, "deployment of a NIT to attempt to identify actual IP addresses…is *the only available* investigative technique with a reasonable likelihood of securing the evidence necessary to prove beyond a reasonable doubt the identity of the TARGET SBUJECTS." Exh. B at ¶ 58 (emphasis added). In the government's own words, then, but for the NIT warrant, they would not have obtained Mr. Hammond's alleged IP address. Thus, this information was not available through some other means.

As a result, Mr. Hammond has thus shown that he was prejudiced by the Rule 41 violation and suppression is therefore an appropriate remedy.

3. The Government Intentionally and Deliberately Disregarded the Jurisdictional Limitations of Rule 41.

Finally, suppression is appropriate because the government deliberately disregarded the jurisdictional limitations of Rule 41(b). The fact that almost every district court to consider this NIT warrant has found it to be unauthorized under Rule 41(b) underscores how clearly Rule 41(b) prohibited the search that the government undertook here.

At the time the government applied for the NIT warrant in February 2015, several courts had ruled that a violation of Rule 41(b)'s territorial limitations could lead to suppression of evidence. The D.C. Circuit's decision in *Glover*, which suppressed a wiretap issued in one district and executed in another as a violation of Rule 41(b), was decided in 2013. *See Glover*, 736 F.3d at 514-15. Although the Tenth Circuit had not decided *Krueger* yet, the district court's opinion—which suppressed evidence seized from a warrant issued in Kansas but executed in Oklahoma—had been decided in February 2014. *See United States v. Krueger*, 998 F.Supp.2d 1032 (D. Kan. 2014).

Most pertinent here, at least one magistrate judge had expressed concerns about its authority to issue a similar warrant to deploy computer code as violating the territorial limits of Rule 41. In 2013, Magistrate Judge Stephen Smith of the Southern District of Texas issued an opinion rejecting the government's request for a search warrant that was remarkably similar to the NIT warrant. *See In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp.2d 753 (S.D. Tex. 2013). The government sought a search warrant that would "surreptitiously install data extraction software on the Target Computer" which, once installed, "has the capacity to search the computer's hard drive, random access memory, and other storage media; to activate the computer's built-in camera; to generate latitude and longitude coordinates for the computer's location; and to transmit the extracted data to FBI agents within this district." *In re Warrant*, 958 F. Supp.2d at 755. The government acknowledged that they did not know the location of the suspects or their computer. Judge Smith denied the warrant, noting that he had no authority under Rule 41(b) to issue a warrant because it was possible the computer would be outside of the Southern District of Texas. *Id.* at 756-58, 761.

Thus, in February 2015 the government was on notice that courts disapproved of the government violating the jurisdictional limitations of Rule 41. The fact that the government went ahead and sought out the NIT warrant anyway—particularly after the concerns articulated by Magistrate Judge Smith in 2013—demonstrates that its violation of Rule 41(b) was intentional and deliberate and warrants suppression.

C. **The Fruits of the NIT Warrant, Specifically the Richmond Search Warrant, Mr. Hammond's Statements to the FBI in July 2015 and the Items Seized and Searched in July 2015 and March 2016, Must Also Be Suppressed.**

The Rule 41(b) violations require suppression of not only the NIT warrant, but all other evidence "obtained as a product of illegal searches and seizures." *United States v. Crawford*, 372 F.3d 1048, 1054 (9th Cir. 2004) (en banc) (citing *Wong Sun v. United States*, 371 U.S. 471, 484-88 (1963)). That extends to evidence seized pursuant to a search warrant that was a "fruit" of the original illegal search. *See United States v. Duran-Orozco*, 192 F.3d 1277, 1281 (9th Cir. 1999).

Here, as explained in detail above, the Richmond search warrant—and the subsequent seizure and search of Mr. Hammond's computer—as well as the statements[9] Mr. Hammond made to the FBI in July 2015 are the "fruit" of the illegal NIT warrant. In turn, the search of Mr. Hammond that took place following his arrest in March 2016, as well as the seizure of any cell phone or computer and the search items after his arrest, are fruits of the Richmond search warrant. Because the NIT warrant is invalid, all these fruits of that initial illegal search must be suppressed as well.

CONCLUSION

For the reasons stated above, the NIT search warrant violated Rule 41 and should be suppressed. Since the Richmond warrant, the items seized from that search—including computers and other property taken from Mr. Hammond in July 2015 and March 2016—and Mr. Hammond's July 2015 statements to the FBI are fruits of the invalid NIT search warrant, those items must be suppressed as well.

DATED: June 2, 2016

STEVEN G. KALAR
Federal Public Defender

/S/
HANNI M. FAKHOURY
Assistant Federal Public Defender

[9] Mr. Hammond may file a subsequent motion to suppress the statements he made to the FBI in July 2015 on Fifth Amendment grounds. Defense counsel received a recording of the interview on May 31, 2016 and needs additional time to review that statement before deciding whether to bring a motion to suppress.