IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA

v. Case No. 17-cr-11-wmc

BRIAN SAVAGE,

Defendant.

UNITED STATES RESPONSE TO DEFENDANT'S MOTION TO EXCLUDE EVIDENCE AND DISMISS THE INDICTMENT

The defendant, Brian Savage, has moved to exclude evidence of child pornography found on his computer. He claims the evidence is the result of an unreasonable search under the Fourth Amendment. U.S. Const. amend. IV. He also moves to dismiss the indictment, claiming the government's conduct violated the Reasonableness Clause of the Fourth Amendment and the Due Process Clause of the Fifth Amendment. U.S. Const. amends. IV, V. The evidence should not be excluded and the indictment should not be dismissed because Savage's consent attenuated the use of a Network Investigative Technique (NIT) from the search of his computer. Assuming for the sake of argument only that it did not, the NIT warrant was valid and the execution of the NIT warrant was reasonable.

I. Introduction

After a months-long investigation, the Federal Bureau of Investigation (FBI) briefly assumed control of Playpen, a website dedicated to child pornography

distribution, for approximately two weeks. On February 20, 2015, the FBI sought and obtained a warrant permitting it to deploy a NIT, which searched computers logging into Playpen for identifying information, including concealed Internet Protocol (IP) addresses. Among the IP addresses identified was one associated with Brian Savage.

On March 16, 2016, more than a year after the NIT warrant was obtained, FBI Special Agents (SAs) Jason Pleming and Forrest Wilkins went to Brian Savage's place of employment to interview him.[1] He agreed to speak to the agents. The officers asked Savage if he was familiar with the Tor network, and he said that he was not. The officers then told Savage that one of his former IP addresses had been linked to child pornography. Savage denied any involvement, asking if he had been framed. The agents presented Savage with a printout containing Savage's username, "sirsavage," as well as details of his online-activity. Savage asked again if he was being framed.

SA Pleming then admonished Savage and told him that lying to federal agents was a crime. Savage again denied he accessed the website, but then asked to speak to SA Pleming alone. SA Wilkins left, and Savage admitted to SA Pleming that he had been accessing child pornography. He said he had a "problem," and his home computer contained approximately forty images and forty videos of child pornography. He signed a consent to search form (see Exhibit B) and the agents and Savage drove separately to Savage's house. Savage led the agents inside his home to his computer, and he explained how to access the files (See Exhibit C).

1 All facts regarding the agents' contact with Savage come from SA Pleming's report attached as Exhibit A.

Savage now moves to suppress all of the images and videos found on his computer because he claims the NIT warrant was invalid. He also asks the Court to dismiss his indictment because he claims the government's conduct was outrageous.

II. Background

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

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

Playpen operated on the anonymous Tor network. The U.S. Naval Research Laboratory created Tor as a means of protecting government communications. It is now available to the public. The Tor network—and the anonymity it provides—is a powerful tool for those who wish to share ideas and information, particularly those living in places where freedom of speech is not accorded the legal protection it is here. But this anonymity has a downside. The Tor network is a haven for criminal activity in general, and for 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 July 7, 2017).

Use of the Tor network masks the user's actual IP address, which could otherwise be used to identify a user, by bouncing user communications around a network of relay computers (called "nodes") run by volunteers.[2] To access the Tor network, users must install Tor software either by downloading an add-on to their web browser or the free "Tor browser bundle." Users can also access Tor through "gateways" on the open Internet that do not provide users with the full anonymizing benefits of Tor. When a Tor user visits a website, the IP address visible to that site is that of a Tor "exit node," not the user's actual IP address; Tor is designed to prevent tracing the user's actual IP address back through that Tor exit node. Accordingly, traditional identification techniques used by law enforcement on the open Internet are not viable.

Within the Tor network itself, certain websites, including Playpen, operate as "hidden services." Like other websites, they are hosted on computer servers that communicate through IP addresses. They operate the same as other public websites with one critical exception: namely, the IP address for the web server is hidden and replaced with a Tor-based web address. This web address is a series of sixteen algorithm-generated characters followed by the suffix ".onion." A user can only reach a "hidden service" by using the Tor client and operating in the Tor network. Unlike an

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

open Internet website, it is not possible to use public lookups to determine the IP address of a computer hosting a "hidden service."

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

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

Acting on a tip from a foreign law enforcement agency as well as information from its own investigation, the FBI determined the computer server that hosted Playpen was located at a web-hosting facility in the United States. In February 2015, FBI agents apprehended the administrator of Playpen and seized the website from its web-hosting facility. Rather than immediately shut the site down, which would have allowed the users of Playpen to go unidentified (and un-apprehended), the FBI

allowed it to continue to operate at a government facility in the Eastern District of Virginia from February 20, 2015, through March 4, 2015.

The FBI obtained court authorizations from the United States District Court for the Eastern District of Virginia to (1) monitor the site users' communications, and (2) deploy a Network Investigative Technique on the site. These tools were used to identify registered users who were anonymously engaging in the sexual abuse and exploitation of children, and to locate and rescue children from the imminent harm of ongoing abuse and exploitation. The NIT warrant affidavit explicitly stated that the FBI would be taking over Playpen and operating it from a server in the Eastern District of Virginia during the period of authorization. (R. 13-1, pgs. 22-23, ¶ 30). Using the NIT, the FBI identified an IP address associated with Brian Savage, which led them to approach him and request an interview.

B. Based on the nature of Playpen and the Tor network, law enforcement sought and obtained court approval to deploy a NIT to identify criminals engaged in the creation, advertisement, and distribution of child pornography.

The 31-page NIT search warrant affidavit was sworn to by a veteran FBI agent with 19 years of federal law enforcement experience and particular training and experience investigating child pornography and the sexual exploitation of children. (R. 13-1, pg. 5, ¶ 1). The affidavit 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. Those users were using anonymizing technology to conceal online child sexual exploitation on a massive scale.

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

In recognition of the technical and legal complexity of the investigation, the NIT warrant affidavit included: a three-page explanation of the offenses under investigation, (R. 13-1, pgs. 6-8, ¶ 4); a seven-page section setting out definitions of technical terms used in the affidavit, (Id., pgs. 8-14, ¶ 5); and, a three-page explanation of the Tor network, how it works, and how users could find a hidden service such as Playpen, (Id., pgs. 14-17, ¶¶ 7-10). The affidavit spelled out the numerous affirmative steps a user would have to go through just to find the site. The agent explained:

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

(Id., pgs. 16-17, ¶ 10). Thus, the agent continued, "[a]ccessing [Playpen] . . . requires numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble upon [it] without understanding its purpose and content." (Id.).

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

The affidavit also described in great detail and in stark terms the purpose of Playpen and why its users were appropriate targets for the NIT. Playpen was "dedicated to the advertisement and distribution of child pornography," "discussion of . . . methods and tactics offenders use to abuse children," and "methods and tactics offenders use to avoid law enforcement detection while perpetrating online child sexual exploitation crimes." (R. 13-1, pg. 14, ¶ 6). More to the point, "administrators and users of [Playpen] regularly sen[t] and receive[d] illegal child pornography via the website." Id. The agent also addressed the sheer scale of the illicit activity occurring on Playpen: site statistics as of February 3, 2015, for Playpen - which was believed to have been in existence only since August of 2014 - showed that it contained 158,094 members, 9,333 message threads, and 95,148 posted messages.[3] (Id., pg. 17, ¶ 11).

Playpen's illicit purpose was also apparent to anyone who visited it during the six months it operated before the FBI seized control of it. "[O]n the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent females with their legs spread apart." (Id., pg. 17, ¶ 12). And the

[3] As the affidavit explained, a bulletin board website such as Playpen is a website that provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. (R. 13-1, pg. 8, ¶ 5(a)).

following text appeared beneath those young girls: "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." While those terms may have seemed insignificant to the untrained eye, the affiant explained, based on his training and his experience, the phrase "no cross-board reposts" referred to a "prohibition against material that is posted on other websites from being 're-posted'" to Playpen and that ".7z" referred to a "preferred method of compressing large files or sets of files for distribution." (Id., pgs. 17-18, ¶ 12). The combination of sexualized images of young girls along with these terms of art referencing image posting and large file compression unmistakably marked Playpen as just what it was—a hub for the trafficking of illicit child pornography.

The affidavit also explained that users were required to register an account by creating a username and password before they could access the site and highlighted the emphasis the registration terms placed on users avowing being identified. Users clicking on the "register an account" hyperlink on the main page were required to accept registration terms, the entire text of which was included in the affidavit. (Id., pgs. 17- 19, ¶¶ 12-13). Playpen repeatedly warned prospective users to be vigilant about their security and the potential of being identified, explicitly stating, "the forum operators do NOT want you to enter a real [e-mail] address," users "should not post information [in their profile] that can be used to identify you," "it is impossible for the staff or the owners of this forum to confirm the true identity of users," "[t]his website is not able to see your IP," and "[f]or your own security when browsing or Tor we also recomend [sic] that you turn off javascript and disable sending of the 'referer' header."

(Id., pgs. 18-19, ¶ 13). This focus on anonymity is entirely consistent with the desire on the part of Playpen administrators and users to evade detection of their illicit activities.

Once a user accepted those terms and conditions, a user was required to enter a username, password, and e-mail address. (R. 13-1, pg. 19, ¶ 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., pgs. 19-21, ¶ 14).

The affidavit also described, in graphic detail, particular child pornography that was available to all registered users of Playpen, including images of prepubescent children and even toddlers being sexually abused by adults. (Id., pgs. 21-22, ¶ 18). Although the affidavit clearly stated that "the entirety of [Playpen was] dedicated to child pornography," it also specified a litany of site sub-forums which contained "the most egregious examples of child pornography" as well as "retellings of real world hands on sexual abuse of children." (Id., pgs. 24-25, ¶ 27).

The affidavit further explained how Playpen 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 and exploitation, including an example where one user wrote to another, "I can help if you are a teen boy and want to fuck your little sister, write me a private message." (Id., pgs. 23-24, ¶ 21). Based on the affiant's training and experience and law enforcement's review of the site, the affiant stated his belief that the site's private message function was being used to "communicate regarding the dissemination of child pornography." (Id., pg. 23, ¶ 22). The affidavit also noted Playpen included multiple

other features intended to facilitate the sharing of child pornography, including an image host, a file host, and a chat service. (Id., pgs. 23-24, ¶¶ 23-25). All of those features allowed site users to upload, disseminate, and access child pornography. In addition, the affidavit included detailed examples and graphic descriptions of prepubescent child pornography disseminated by site users through each one of those features. (Id.).

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

The NIT warrant affidavit contained a detailed and specific explanation of the NIT, its necessity, how and where it would be deployed, what information it would collect, and why that information constituted evidence of a crime.[4]

Specifically, the affidavit noted that without the use of the NIT "the identities of the administrators and users of [Playpen] would remain unknown" because any IP address logs of user activity on Playpen would consist only of Tor "exit nodes," which "cannot be used to locate and identify the administrators and users." (R. 13-1, pg. 26, ¶ 29). Further, because of the "unique nature of the Tor network and the method by which the network . . . route[s] communications through multiple other computers, . . .

[4] Savage describes the NIT as "malware." (R. 12, pgs. 1, 2). That label is unhelpful to the Court's analysis. As discussed herein, the NIT is a legitimate law enforcement tool. Here, its use was judicially authorized based on a showing of probable cause. ("NITs, while raising serious concerns, are legitimate law enforcement tools." *United States v. Levin*, No. 15-CR-10271, 2016 WL 2596010 at *14 (D. Mass. May 5, 2016)). It consisted of computer instructions designed to cause the user's computer to transmit a limited set of information to assist in identifying the computer used to access Playpen and its user. Indeed, as one court observed in dismissing the defendant's characterization of the NIT as malware: "perhaps malware is a better description for the program through which the provider of the pornography attempted to conceal its distribution of contraband over the Internet than for the efforts of the Government to uncover the pornography." *United States v. Matish*, 190 F. Supp. 3d 585, 601-02 (E.D. Va. June 23, 2016).

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 if they are tried." (Id., pgs. 27-28, ¶ 31). The affiant thus concluded, "using a NIT may help FBI agents locate the administrators and users" of Playpen. (Id., pgs. 27-28, ¶¶ 31-32). Indeed, he explained, based upon his training and experience and that of other officers and forensic professionals, the NIT was a "presently available investigative technique with a reasonable likelihood of securing the evidence necessary to prove . . . the actual location and identity" of Playpen users who were "engaging in the federal offenses enumerated" in the warrant. (Id., pg. 27, ¶ 31).

In terms of the deployment of the NIT, the affidavit explained that when a user's computer downloads site content in the normal course of operation, the NIT would augment the content with additional computer instructions. (Id., pg. 28, ¶ 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 discrete pieces of information to be collected were detailed in the NIT warrant and accompanying Attachment B, along with technical explanations of the terms. They were limited to the following: (1) the actual IP address assigned to the user's computer; (2) a unique identifier to distinguish the data from that collected from other computers; (3) the operating system running on the computer; (4) information about whether the NIT had already been delivered to the computer; (5) the computer's Host Name; (6) the

computer's active operating system username; and (7) the computer's Media Access Control (MAC) address. (Id., pgs. 28-30, ¶ 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., pg. 30, ¶ 35). For instance:

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

(Id.).

The affidavit specifically requested authority to deploy the NIT each time any user logged into Playpen with a username and a password. (Id., pg. 26, ¶ 36). However, the affidavit disclosed to the magistrate that, "in order to ensure technical feasibility and avoid detection of the technique by suspects under investigation," the FBI might "deploy the NIT more discretely against particular users," including those who "attained a higher status" on the site or "in particular areas of [Playpen]" such as the sub-forums with the most egregious activity, which were described elsewhere in the affidavit. (Id., pg. 28, ¶ 32 n.8). Finally, the affidavit requested authority for the NIT to "cause an activating computer—wherever located—to send to a computer controlled by or known to the government . . . messages containing information that may assist in

identifying the computer, its location, other information about the computer and the user of the computer." (Id., pgs. 33-34, ¶ 46(a)).

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

As noted above, among the things described in the NIT warrant affidavit was Playpen's site logo: "on the main page of the site, located to either side of the site name, were two images depicting partially clothed prepubescent females with their legs spread apart." (R. 13-1, pg. 17, ¶ 12). Between September 16, 2014 and February 3, 2015, FBI agents reviewed Playpen in an undercover capacity to document the activity on the site. (Id., pg. 17, ¶ 11). Sometime before February 18, 2015, Playpen's administrator changed the URL—the site address. Noticing the URL had changed, the affiant visited Playpen on February 18, 2015, and confirmed the content had not changed. (Id., pg. 17, ¶ 11 n.3). This includes the site logo.

In the evening of February 19, 2015, the FBI executed a search at the Florida home of the Playpen administrator and apprehended him. (Id., pgs. 26-27, ¶ 30). At that point, the FBI also assumed control of Playpen. Postings by the administrator from earlier in the day show that just before he was arrested, the administrator changed Playpen's site logo, replacing the images described above with a single image showing a prepubescent girl, wearing a short dress and black stockings, reclined on a chair with her legs crossed and posed in a sexually suggestive manner. (R. 13-17). The text described in the affidavit as part of the logo, "[n]o cross-board reposts, .7z preferred, encrypt filenames, include preview," which the affidavit explained pertain to image

distribution, remained unchanged. (*Compare* R. 13-1, pg. 17, ¶ 12 *with* R. 13-16, 13-17). The NIT warrant was sworn to and authorized at 11:45 a.m. on February 20, 2015, the day after the logo change. The affidavit did not reference this recent change.

III. Argument

There is no question information from the NIT warrant led the FBI Special Agents to approach the defendant and question him about his online activities. However, this does not automatically make evidence Savage provided to the agents inadmissible. First, even if the NIT warrant was invalid, Savage's consent to search attenuated the use of the NIT from the search of his computer. Second, the NIT warrant was valid because it was supported by probable cause, described the places to search with particularity, and was within the judge's jurisdiction. Third, the government's execution of the warrant was reasonable under the Due Process Clause of the Fifth Amendment, and under the Reasonableness Clause of the Fourth Amendment.

A. The search of Savage's computer was attenuated from the investigation by Savage's consent to search and, consequently the evidence should not be suppressed.[5]

The evidence obtained in this case was not through a court ordered search warrant, but through Savage's own actions. Because Savage agreed to the search and seizure of his computer, the evidence found on his computer should not be suppressed.

The exclusionary rule requires the suppression of evidence obtained in violation of the Fourth Amendment. The fact that a Fourth Amendment violation has occurred,

5 For the purpose of this section only, the United States assumes the NIT search warrant was invalid.

however, "does not necessarily mean that the exclusionary rule applies." *United States v. Carter,* 573 F.3d 418, 422 (7th Cir. 2009) (quoting *Herring v. United States,* 555 U.S. 135, 141 (2009)). "Indeed, exclusion 'has always been our last resort, not our first impulse.' " *Herring,* 555 U.S. at 140 (quoting *Hudson v. Michigan,* 547 U.S. 586, 591 (2006)). Because the exclusionary rule is a " 'judicially created remedy' whose prime purpose is to deter future unlawful police conduct," *United States v. Fazio,* 914 F.2d 950, 957 (7th Cir. 1990) (quoting *United States v. Calandra,* 414 U.S. 338, 348 (1974)), it "applies only where it 'results in appreciable deterrence.' " *Carter,* 573 F.3d at 422 (quoting *Herring,* 555 U.S. at 141).

The Supreme Court has held that the exclusionary rule does not apply when the connection between the Fourth Amendment violation and the subsequent discovery of evidence "become[s] so attenuated that the deterrent effect of the exclusionary rule no longer justifies its cost." *Brown v. Illinois,* 422 U.S. 590, 609 (1975). For this reason, the Court has declined to adopt a "but for" rule of causation that would render inadmissible all evidence discovered subsequent to an unlawful search. *Carter,* 573 F.3d at 424 (citing *Hudson,* 547 U.S. at 591). Instead, the Court has concluded that the exclusionary rule "should not apply when the causal connection between illegal police conduct and the procurement of evidence is 'so attenuated as to dissipate the taint' of the illegal action." *Fazio,* 914 F.2d at 957 (quoting *Segura v. United States,* 468 U.S. 796, 805 (1984)).

In *Brown*, the Supreme Court set forth several factors to consider in determining "whether the taint of an unlawful search or arrest has sufficiently dissipated so as to no

longer taint a subsequently acquired statement." *Fazio,* 914 F.3d at 957 (quoting *United States v. Patino,* 862 F.2d 128, 132 (7th Cir. 1988)). Under *Brown,* courts look to: (1) the temporal proximity of the illegal conduct to the subsequently obtained evidence or statement; (2) the presence of any intervening circumstances; and (3) the purpose and flagrancy of the official misconduct. *Brown,* 422 U.S. at 603-04. Additionally, in the context of written or oral statements, the voluntariness of the statement under the Fifth Amendment is a "threshold requirement" that must be established prior to undertaking an attenuation analysis. *Brown,* 422 U.S. at 604; *Fazio,* 914 F.2d at 957.

1. Savage's statements were voluntary.

In the context of written or oral statements, the voluntariness of the statement under the Fifth Amendment is a "threshold requirement." *Brown,* 422 U.S. at 602; *Fazio,* 914 F.2d at 957. Although not dispositive, voluntariness is also "an important factor" in the attenuation inquiry. *Fazio,* 914 F.2d at 957.

Savage's consent to the search of his home and his computer was voluntary and there is absolutely no indication otherwise. The government must prove by a preponderance of the evidence that the consent was voluntary. *United States v. Richards*, 741 F.3d 843, 847–48 (7th Cir. 2014). Consent is evaluated based on the following six factors: "(1) the age, education, and intelligence of the individual; (2) whether he was advised of his rights; (3) whether he was in custody; (4) how long the individual was detained prior to consenting; (5) whether consent was given immediately or after several requests; and (6) whether the officers used physical coercion." *United States v.*

Thompson, 842 F.3d 1002, 1009–1010 (7th Cir. 2016). These factors are evaluated based on a totality of the circumstances. *Id.* at 1010.

Mr. Savage was 23 years old at the time of the interview and did not have any intellectual or educational deficit. He was not advised of his *Miranda*[6] rights, but he was also never placed in custody. The interview was consensual and short, and the agents never told Savage that he was not free to leave. In fact, Savage drove his own car from his place of employment to his home to give his computer to the agents. Savage denied involvement three times before he admitted possessing child pornography, but after confessing, Mr. Savage gave consent to search after the first request.

Though courts have been somewhat wary of using illegally-seized evidence to coerce consent, *see United States v. Liss*, 103 F.3d 617, 622 (7th Cir. 1997) (Ripple, J., concurring), the agents in this case presented the information without using it to coerce. They did not make threats, they did not imply his consent to search was unnecessary for their case, and they did not misconstrue any of the circumstances. They simply presented the evidence and then asked if he possessed child pornography. Based on these factors, the consent was voluntary, and the threshold requirement of attenuation has been met.

2. Savage's consent sufficiently attenuated the search of his computer from the NIT warrant.

The first *Brown* factor is the temporal proximity between the Fourth Amendment violation and the challenged evidence or statements. *Brown,* 422 U.S. at 603. The time

6 *Miranda v. Arizona*, 384 U.S. 436 (1966).

span between the violation and the challenged evidence or statement "is not 'dispositive on the question of taint,' " however, and must be considered in light of the circumstances surrounding the acquisition of the evidence or statement and the intervening factors. *Fazio,* 914 F.2d at 957-58 (quoting *Patino,* 862 F.2d at 133 n.3).

Here, the seizure of the defendant's computer and the defendant's statement to agents occurred more than a full year after the NIT warrant was issued. Although there is no bright-line test for determining the lapse of time necessary to purge the taint of an unconstitutional action, a year greatly exceeds what most courts have deemed sufficient. *See, e.g., Rawlings v. Kentucky,* 448 U.S. 98, 107-08 (1980) (holding that 45-minute interval between illegal detention and statement sufficient to purge the taint of the illegal detention when combined with *Miranda* waiver and "congenial atmosphere"); *United States v. Pineda-Buenaventura,* 622 F.3d 761, 777 (7th Cir. 2010) (finding attenuation where consent to search obtained 45 minutes after illegal entry); *Fazio,* 914 F.2d at 957-58 (holding statement made one hour after illegal search was admissible); *United States v. Valencia,* 913 F.2d 378, 382 (7th Cir. 1990) (defendant consented to search one hour after illegal search).

The time between the violation and the acquisition of evidence bears the least weight and is never dispositive. *Carter*, 573 F.3d at 425; *see also United States v. Conrad*, 673 F.3d 728, 738 (7th Cir. 2013) (Tinder, J., dissenting in part). In this case, the length of time between the search and the consent admittedly does not add much to the equation because the typical consideration of the temporal element – did the defendant have time

reflect on his circumstances – did not apply to the defendant who was unaware of the NIT warrant signed a year earlier.

The second *Brown* factor to consider is whether there were any intervening circumstances. *Brown*, 422 U.S. at 603. Intervening circumstances are events that "sever the causal connection" between the violation and the discovery of evidence. *Conrad*, 673 F.3d at 734 (citation omitted). Voluntary consent is not attenuation *per se*, *United States v. Robeles-Ortega*, 348 F.3d 679, 684 (7th Cir. 2003), but it can be an intervening circumstance if not obtained pursuant to an illegal stop, detention, arrest, or entry, *Conrad*, 673 F.3d at 734. Because the test is objective, the motivation of law enforcement in requesting consent is not relevant, even if an illegal search motivated the investigation. *Carter*, 573 F.3d at 427.

Moreover, the valid consent given by Savage makes his statements and the evidence found on his computer admissible, regardless of why the agents went to speak to him in the first place. *Carter*, 573 F.3d at 427, citing *Liss*, 103 F.3d at 621-22 ("a non-custodial voluntary consent should be seen as an independent intervening event behind which we will not probe for improper motivation and which thus serves as a break in any causal chain stemming from an illegal search").

The defendant in *Liss* was charged with selling methamphetamine after police found drugs during a consent search of his home. *Liss*, 103 F.3d at 619-120. Liss argued suppression was warranted because the police only asked to search his home following the illegal search of his barn. *Id*. at 620. His argument was that but for the illegal search, police would have had no reason to suspect him of wrongdoing and ask to

search his home. The Court held that *Liss'* consent to search was a sufficient intervening event to break the chain between the illegal search and the subsequent discovery of the evidence found in his home, reasoning that the police do not need a good reason to ask to search someone's home. *Id.*, at 621 (citing *Florida v. Bostick*, 501 U.S. 429, 434-35 (1991)). *See also Carter*, 573 F.3d at 427. The motivation of the police is "essentially irrelevant because the person asked can always refuse to grant consent and stop the search. 'The fact that an officer had actual suspicion, however obtained, cannot render invalid a consent for which the officer did not need any suspicion at all to request.'" *Carter*, 573 F.3d 427 (quoting *Liss*, 103 F.3d at 621).

Carter reiterated *Liss* did not establish a *per se* rule validating every consent search following a Fourth Amendment violation. *Carter,* 573 F.3d at 427 n. 3. However, in *Carter*, the court said the holding in *Liss* would apply because "consent was given by a person unaware of the earlier warrantless entry, at a different location, and with different police personnel involved." *Id.* The exact same scenario is present in this case – Savage was unaware of the NIT warrant at the time he gave consent, the NIT warrant was executed at a different location, and SAs Wilkens and Pleming were not involved in obtaining the NIT warrant. Thus, Savage's consent made all the subsequent evidence obtained admissible, no matter how the officers got to him.

The final *Brown* factor is the "purpose and flagrancy" of the violation. *Brown,* 422 U.S. at 604. "Because the primary purpose of the exclusionary rule is to discourage police misconduct, application of the rule does not serve this deterrent function when the police action, although erroneous, was not undertaken in an effort to benefit police

at the expense of the suspect's protected rights." *Fazio,* 914 F.2d at 958. Accordingly, "[w]here the police erred but the record does not support an inference of bad faith [ ], the violation was not flagrant." *Carter,* 573 F.3d at 425-26.

This factor also favors attenuation. The investigators identified Savage based on a search warrant authorized by a neutral magistrate judge, and they interviewed Savage with his consent. They sought specific types of files from his computer, and they seized those files with Savage's consent.

Moreover, at the time the officers approached Savage, no court had ruled that evidence from the NIT warrant should be suppressed.[7] It appears the first time that occurred was May 5, 2016. *See United States v. Levin,* No. CR 15-10271, 2016 WL 2596010 (D. Mass. May 5, 2016). Therefore, the agents did not opt to seek consent for any nefarious purpose, such as to skirt a warrant they knew was invalid.

3. The lack of a deterrent effect on police favors admission of evidence based on public policy.

The three-factor test points in favor of attenuation, and the purpose of the exclusionary rule does as well. Evidence obtained through government misconduct is excluded to deter future misconduct. *Conrad*, 673 F.3d at 732. Where exclusion will not deter misconduct, the costs of suppressing evidence and risking that a guilty person will go free may outweigh the court's interest in deterrence. *Utah v. Strieff*, 136 S. Ct.

---

7 Prior to that date, three district courts had held that the warrant was improperly issued but that suppression was unwarranted. *See United States v. Machaud*, No. 3:15-cr-05351-RJB, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016); *United States v. Stamper*, No. 1:15cr109, 2016 WL 695660 (SD. Ohio Feb. 19, 2016); and *United States v. Epich*, No. 15-cr-163-PP, 2016 WL 953269 (E.D. Wis. March 14, 2016).

2056, 2061 (2016). Even if the NIT warrant was invalid, suppression would have little deterrent effect on the FBI in this case. The investigators only acted upon the issuance of a warrant, and they presented the judge with all relevant information when applying for the warrant. Even if the magistrate judge issued a warrant beyond her jurisdiction, the exclusion of evidence would not change the behavior of the police, and it would allow participants in a child pornography forum to go free. Consequently, the exclusion of evidence is not appropriate in this case.

B. The NIT warrant was valid and did not violate Savage's Fourth Amendment rights.

As a preliminary matter, as discussed below (see pages 42-44) Savage had no expectation of privacy in his IP address, particularly because the IP address only identified the defendant. The actual search of his computers contents was, as discussed above, based solely on his consent. Because Savage had no expectation of privacy in his IP address, a warrant to capture it was not even needed and no further analysis of the warrant need be completed.

Assuming for the sake of argument only that the underlying NIT warrant must be analyzed and evaluated in this case, the evidence was still lawfully obtained. The defendant makes two general arguments in favor of unlawful seizure. First, he argues the government violated the Warrant and Reasonableness Clauses of the Fourth Amendment. To support this, he claims the warrant lacked particularity, law enforcement victimized the children portrayed on the website, and the NIT failed to communicate its scope to the magistrate judge, resulting in a warrant void *ab initio*. Finally, he claims the warrant was not supported by probable cause, particularly when

omitted facts are considered. The defendant's second general argument is that his Due Process rights were violated due to the government's alleged outrageous government conduct. (R. 12, pgs. 23-24). As detailed below, none of these arguments have merit and the defendant's motion should be denied.

1. The NIT warrant stated the locations to be searched with particularity.

Savage contends the NIT warrant was unconstitutional because it "described the place to be searched in ambiguous terms and its affidavit discussed the agents' intent to exercise discretion to decide which computers to search and how many times to search them." (R. 12, pg. 7). However, the NIT warrant described specifically the places to be searched - activating computers of users or administrators that logged into Playpen - and the things to be seized - the seven pieces of information obtained from those activating computers. And a neutral and detached judge found there was probable cause to support the requested search. The Fourth Amendment requires no more.

The NIT warrant described the locations to be searched with particularity. The constitutional principles at play here are well-settled. "[N]o warrants shall issue, but upon probable cause, . . . and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The Constitution demands that two things be described with particularity: "'the place to be searched' and 'the persons or things to be seized.'" *United States v. Grubbs*, 547 U.S. 90, 97 (2006) (citation omitted).

As to the place, "[t]he basic requirement is that the officers who are commanded to search be able from the 'particular' description of the search warrant to identify the specific place for which there is probable cause to believe that a crime is being

committed." *United States v. White*, 416 F.3d 634, 637 (7th Cir. 2005) (citation omitted). As to the items to be seized, nothing must be "left to the discretion of the officer executing the warrant" in deciding what to seize. *Marron v. United States*, 275 U.S. 192, 196 (1927). Whether this particularity standard is met is determined in light of the information available at the time the warrant issued. *White*, 416 F.3d at 637–38 (citing *Maryland v. Garrison*, 480 U.S. 79, 85 (1987)).

The NIT warrant meets both requirements through Attachments A and B of the NIT warrant, respectively, identified the "Place to be Searched" and the "Information to be Seized." Both defined with precision where agents could look and for what. The warrant authorized deployment of the NIT to the computer server hosting Playpen and then to computers of "any user or administrator who logs into [Playpen] by entering a username and password." (R. 13-1, pg. 3, Att. A). Attachment B, in turn, imposed precise limits on what information could be obtained from those computers by the NIT: the seven pieces of information listed. (Id., pg. 4, Att. B).[8]

Savage contends that the warrant did not state the agents' intentions to search 50,000 computers located worldwide. To be sure, the Fourth Amendment demands that there be probable cause to search a particular location for particular items. But the notion that a warrant supported by sufficient probable cause to authorize a search of numerous locations is, for that reason alone, constitutionally defective is absurd. Either

8 The defendant's claim that the affidavit was not incorporated into the warrant is refuted by the warrant, which indicates the issuing court "find(s) the affidavit(s), or any recorded testimony, establish(es) probable cause to search and seize the person or property." (R. 13-1, pg. 2).

probable cause exists to support a search or searches or it does not. As discussed below, here the affidavit establishes probable cause to believe that anyone who logged into Playpen did so with knowledge of its content and the intent to consume it. Accordingly, the warrant properly authorized the deployment of the NIT to any such user, regardless of how many there are or could be.

Savage contends that the NIT warrant did not authorize multiple searches of the same computer. However, Savage does not allege that the NIT was deployed multiple times against him, so whether multiple deployments of the NIT were allowed or would have been a Fourth Amendment violation is not at issue.

Savage also contends that the deployment of the NIT against only some of the computers authorized by the warrant leaves the scope of the search at the discretion of the investigators. However, the scope of the search was limited to activating computers on the server, and the fact that probable cause to search existed for thousands of computers does mean that the warrant lacked particularity. *See United States v. Broy*, 209 F. Supp. 3d 1045, 1051 (C.D. Ill. Sept. 21, 2016). A warrant is "facially deficient" only when it fails to provide any meaningful instruction to the search agents regarding the items to be seized. *See Marron*, 275 U.S. at 196. The fact that 50,000 computers per week fell within the scope of the search merely indicated a large amount of criminal activity. That the FBI retained discretion to execute the warrant on a narrower set of users does not somehow convert it into an unconstitutional general warrant.

To the extent that Savage claims that the warrant lacked particularity as to how the NIT would work, his argument also fails. *See United States v. Rigmaiden*, 2013 WL

1932800 *16 (D. Arizona, May 8, 2013) (rejecting argument that tracking warrant was insufficiently particular even where warrant did not describe "the precise means by which the . . . device would operate."). There is no legal requirement that a search warrant specify the precise manner in which the search is to be executed. *Dalia v. United States*, 441 U.S. 238, 257 (1979); *see also Garrison*, 480 U.S. at 84. "The fourth Amendment . . . does not set forth some general 'particularity requirement.' It specifies only two matters that must be 'particularly describ[ed] in the warrant: 'the places to be searched' and 'the persons or things to be seized.'" *Grubbs*, 547 U.S. at 97 (citing *Dalia*, 441 U.S. at 257).

2. The government's conduct was reasonable.

According to the defendant, the second problem with the NIT warrant was that it victimized the children depicted in the images, and thus violated the Reasonableness Clause. (R. 12, pgs. 10-14). Given the nature of child pornography investigation, the maintenance of the website during the Playpen investigation was reasonable. Possession, receipt, and distribution of child pornography can have a direct, "haunt[ing]" harm to the child portrayed. *United States v. Sherman* 268 F.3d 539, 547 (7th Cir. 2001) (citation omitted). *See also Paroline v. United States*, 134 S. Ct. 1710, 1727 (2014). Savage claims that the government re-victimized the children portrayed in the pornography in Playpen by maintaining the site, and that in doing so they violated the Reasonableness Clause of the Fourth Amendment.

However, in order to combat human trafficking, sexual abuse, and the distribution of large amounts of child pornography, the investigators, based on their

experience, found it necessary to maintain the site until they could identify its members and administrators. The investigators limited the time the site remained online, shut down the section of the site that encouraged production of new content, and monitored the site for new content in order to prevent ongoing child abuse. This course of action was described in the warrant application and approved by a federal magistrate judge. The government did not encourage Savage to use child pornography, and Savage himself was not harmed by the alleged misconduct. Consequently, the investigation was not unreasonable under the Fourth Amendment.

In short, this argument is nothing more than an argument that the government acted outrageously, and as discussed in detail below (see pages 52-54) this argument is not recognized in the Seventh Circuit.

3. The NIT warrant was not void *ab initio* due to a lack of jurisdiction by the issuing judge.

The defendant next argues the warrant was void *ab initio* because the issuing judge lacked jurisdiction. Perhaps recognizing that even if a violation of 41(b) occurred, it does not implicate the Fourth Amendment, the defendant attempts to argue some sinister motive by the Department of Justice, claiming DOJ attorneys "hid the ball" from the magistrate by the failure to include a clear and accurate description of the places to be searched. (R. 12, pg. 16).

This argument fails for numerous reasons. First, as described above, the warrant does include a clear and accurate description of the places to be searched. There was no "hiding the ball." Second, the United States asserts the NIT was authorized by Rule 41.

Finally, this argument is flawed because it equates Rule 41(b)'s venue provisions with the Fourth Amendment's warrant requirements.

i. The NIT was authorized by Rule 41

While different courts have come to different conclusions, the United States continues to assert the NIT Warrant was validly issued pursuant to Rule 41(b). Rule 41(b)(4) authorized the magistrate judge in the Eastern District of Virginia to issue a warrant to install the NIT on the government-controlled Playpen server located within the district, and that warrant properly authorized use of the NIT to track the movement of information - the digital child pornography content requested by users who logged into Playpen's website - as it traveled from the server in the Eastern District of Virginia through the encrypted Tor network to its final destination: the users' activating computers, wherever located. At that point, the NIT caused the activating computers to transmit specified network information back to the government over the open Internet, thus enabling the government to locate and identify the user. *See United States v. Johnson*, No. 15-cr-00340, 2016 WL 6136586, at **3-7 (W.D. Mo. Oct. 20, 2016) (NIT Warrant authorized under Rule 41(b)(4)); *United States v. Jean*, 207 F. Supp. 3d 920, 942-943 (W.D. Ark. 2016) (same); *United States v. Eure*, No. 2:16-CR-43, 2016 WL 4059663, at *8 (same); *United States v. Darby*, 190 F. Supp. 3d 520, 536-37 (E.D. Va. 2016) (same); *United States v. Matish*, 193 F. Supp. 3d 585, 612 (E.D. Va. 2016) (same).

The Supreme Court has urged a "flexible" interpretation of Rule 41 "to include within its scope electronic intrusions authorized upon a finding of probable cause." *United States v. New York Tel. Co.*, 434 U.S. 159, 169 & n.16 (1977) (upholding a 20-day

search warrant for a pen register to collect dialed telephone number information, despite the fact that Rule 41's definition of "property" did not, at that time, include such information and required that a search be conducted within 10 days). The Supreme Court explained that its flexible reading of Rule 41 was "reinforce[d]" by Rule 57(b), which provides, "[i]f no procedure is specifically prescribed by rule, the court may proceed in any lawful manner not inconsistent with these rules or with any applicable statute." *New York Tel. Co.*, 434 U.S. at 170 (citing Fed. R. Crim. P. 57(b)). Stated another way, when presented with a constitutionally valid, and not statutorily prohibited, request for a search warrant, courts are empowered to read the language of Rule 41 broadly in determining whether the requested search falls within its scope. *Id.*; *see also United States v. Torres*, 751 F.2d 875, 878 (7th Cir. 1984).

Rule 41(b)(4) allows a magistrate judge "to issue a warrant to install within the district a tracking device," which may be used "to track the movement of a person or property located within the district, outside the district, or both." The Rule defines a "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. §3117(b); *see* Fed. R. Crim. P. 41(a)(2)(E) (incorporating this definition). The Rule further defines "property" to include not only "tangible objects," but also "information." Fed. R. Crim. P. 41(a)(2)(A). Although the term "device" is not more specifically defined in the Rule, it is a word commonly used to describe "[a] thing made or adapted for a particular purpose." Oxford English Dictionary, https://en.oxforddictionaries.com/definition/device (last visited January 15, 2017).

Applying these definitions, the NIT qualifies as a "tracking device" within the meaning of Rule 41(b)(4).[9] As applied to older technologies, the Rule contemplates that a tracking device may be a mechanical tool used to track the movement of a tangible object - *e.g.*, a transmitter affixed to a container of chloroform placed in a vehicle traveling over public roadways, like the beeper in *United States v. Knotts*, 460 U.S. 276 (1983). As applied to newer technologies, the Rule envisions that a tracking device may be an electronic device used to track the movement of information - *e.g.*, computer instructions embedded in digital content traveling on data highways, like the NIT in this case. The NIT comprised a set of "computer instructions" "designed to cause the user's 'activating' computer to transmit certain information to a computer controlled by or known to the government." (R. 13-1, pg. 28, ¶33). The NIT would "augment" the digital content requested by Playpen users and, once a user's computer downloaded the requested content and the NIT, the NIT would "reveal to the government environmental variables and certain registry-type information that may assist in identifying the user's computer, its location, and the user of the computer." (Id., pgs. 28-29, ¶¶33-34).

Essentially, the NIT was designed to follow illegal child pornography content requested by a user who accessed Playpen in the Eastern District of Virginia, through the anonymous Tor network nodes, and back to the user's activating computer; at that point, the NIT caused the transmission of the location-identifying information back to

9 The United States understands that this Court has already found this to be a fair, but ultimately unpersuasive argument. *United States v. Johnson,* 16-cr-76, R. 28, Report and Recommendation, pg. 24.

the government over the open Internet, thus circumventing Tor's encryption and allowing the government to identify and locate the user. Similar to a transmitter affixed to an automobile that is programmed to send location-enabling signals (like GPS coordinates) back to a government-controlled receiver at pre-determined intervals, the NIT augmenting the digital content requested by a Playpen user was designed to send location-enabling information (like an actual IP address) back to a government-controlled computer when the illegal child pornography content reached its ultimate destination - the user's activating computer. Thus, although not a physical beeper affixed to a tangible object, the NIT operated as a digital tracking device of intangible information within the meaning of Rule 41(b)(4).

The NIT was installed in the Eastern District of Virginia, as required by Rule 41(b)(4). Subdivision (4) authorizes a magistrate judge to issue a warrant "to install within the district a tracking device." The record establishes that the NIT was installed in the Eastern District of Virginia and only moved outside the district after a Playpen user entered the district to retrieve the illegal website content it augmented. Agents deployed the NIT alongside Playpen's digital content on the government-controlled server in the Eastern District of Virginia. (R. 13-1, pg. 28, ¶32). This deployment constituted installation of a tracking device under Rule 41, as users then retrieved the NIT from the Playpen server by logging on and downloading information from that server. Any person seeking to access Playpen's child pornography content thus had to make, "in computer language, 'a virtual trip' via the Internet to Virginia," where the server was located. *Matish*, 193 F. Supp. 3d at 612; *United States v. Dzwonczyk*, No. 4:15-

CR-3134, 2016 WL 7428390 at *13 (D. Neb. Dec. 23, 2016) (same); *Darby*, 190 F. Supp. 3d at 536 ("Users of Playpen digitally touched down in the Eastern District of Virginia when they logged into the site."); *see also Jean*, 207 F. Supp. 3d at 942; *Johnson*, 2016 WL 6136586, at*6. When an individual entered his username and password on the Playpen website, it triggered installation of the NIT; both of these actions occurred in the Eastern District of Virginia. (R. 13-1, pg. 28, ¶33). In sum, the NIT was installed for purposes of Rule 41's tracking device provision at the location where it was obtained by a Playpen user (the Playpen server in the Eastern District of Virginia), not where the NIT ultimately disclosed the location-identifying information (the user's computer). The NIT thus complied with Rule 41(b)(4)'s installation requirement.

In sum, Rule 41(b)(4) authorized the magistrate judge in the Eastern District of Virginia to issue the NIT Warrant, and to the extent the Court finds any ambiguity in the tracking device provision, Rule 41 must be read flexibly to accommodate the use of new law enforcement techniques necessary to unearth electronic evidence and ferret out criminals cloaked by anonymizing software. Because the magistrate judge validly exercised her authority to issue the NIT Warrant, the evidence obtained therefrom is admissible against Savage.

ii. Even if a violation of 41(b) occurred, it is not of constitutional dimension.

Savage also argues the warrant is void *ab initio,* because Judge Buchanan was not authorized to issue a warrant in Wisconsin. This argument is flawed because it equates Rule 41(b)'s venue provisions with the Fourth Amendment's warrant requirements.

The requirements of Rule 41 and the Fourth Amendment are not coextensive. *See United States v. Schoenheit*, 856 F.2d 74, 77 (8th Cir. 1988). Rule 41(b) places limits on the territorial authority of magistrate judges to issue certain types of warrant, and the Fourth Amendment says nothing about where the magistrate's authority may be exercised. Here, the NIT warrant was issued by a neutral and detached, duly appointed magistrate judge, who determined the warrant was supported by probable cause and particularly described the place to be searched and things to be seized; it was, therefore, judicially approved for Fourth Amendment purposes. *See United States v. Knowles*, 207 F. Supp. 3d 595, 601 (DSC 2016) ("Because Magistrate Judge Buchanan was a neutral and detached judicial officer, authorized to issue search warrants and capable of determining whether probable cause existed, her approval of the search warrant was constitutionally sufficient judicial approval."). *See, e.g.*, *United States v. Allain*, 213 F. Supp. 3d 236, 251 n.8 (D.Mass. 2016) (describing Rule 41(b) violation as running "afoul of a jurisdictional statute" and not "of constitutional dimension"); *United States v. Anzalone*, 208 F. Supp. 3d 358, 371 (D. Mass. 2016) (finding Rule 41(b) violation non-constitutional); *Johnson*, 2016 WL 6136586, at *7; *Knowles*, 207 F. Supp. 3d at 600-01; *Jean*, 207 F. Supp. 3d at 943-44; *United States v. Henderson*, No. 15-cr-565-WHO-1, 2016 WL 4549108, at *5 (N.D. Cal, Sept. 1, 2016); *United States v. Adams*, No. 6:16-cr-11-Or;-40GJK, 2016 WL 4212079, at *7 (M.D. Fla. Aug. 10, 2016); *United States v. Acevedo-Lemus*, No. SACR 15-137-CJC, 2016 WL 4208436, at *7 (C.D. Cal., Aug. 8, 2016); *Matish*, F. Supp. 3d at 622; *United States v. Werdene*, 188 F. Supp. 3d 342, 446-47 (E.D. Pa. 2016); *United States v. Michaud*, No. 3:15-cr-05.51-RJB, 2016 WL 337263, at **6-7 (W.D. Wash., Jan. 28, 2016).

A rule 41(b) error in this case, if it occurred, was technical or ministerial and not of constitutional dimension and suppression is not justified.[10]

Additionally, the Seventh Circuit has held "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). Suppression of evidence is rarely, if ever, the remedy for a violation of Rule 41, even if such a violation has occurred. *Id.* (citing *United States v. Berkos*, 543 F.3d 392, 396 (7th Cir. 2008)).

iii. If a showing of prejudice is required, Savage was not prejudiced

Part of the defendant's suppression argument relies on *United States v. Krueger*, 809 F.3d 1109 (10th Cir. 2015). (R. 12, pg. 17). There, the district court suppressed evidence of child pornography after agents secured a warrant from a magistrate judge in Kansas that had explicitly requested authorization to search a home in Oklahoma. *Id.* at 1111. On appeal, the government conceded the warrant plainly violated Rule 41(b) and did not argue the good faith exception applied. *Id.* at 1113. The government suggested a prejudice inquiry that "asked whether any federal magistrate judge in the Western District of *Oklahoma*, the district within which [the targeted] residence [was] located, could have issued" the warrant. *Id.* at 1116. But *Krueger* rejected that approach.

[10] The government also relies on *United States v. Dzwonczyk*, No. 4:15-CR-3134, 2016 WL 7428390, at *2 (D. Neb. Dec. 23, 2016); *United States v. Duncan*, 15-CR-414, 2016 WL 7131475 (D. Or. Dec. 6, 2016); *United States v. Stepus*, 15-CR-20038, 2016 WL 6518427, at *2 (D. Mass. Oct. 28, 2016); *United States v. Anzalone*, 208 F. Supp. 3d 358, 372 (D. Mass. Sept. 22, 2016), for holding that NIT search warrant was not void *ab initio* because it was valid at least in the district where it was issued.

Krueger is at best difficult, if not impossible to square with the Seventh Circuit cases that hold "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." *Cazares-Olivas*, 515 F.3d at 730. Prejudice necessarily would always be established under *Krueger*, but the Seventh Circuit has rightly determined such errors could be nonprejudicial.[11]

Moreover, *Krueger* "expressly [did] not address the propriety of suppression when, at the time of issuance, *it is genuinely unclear*, whether the federal magistrate judge has authority to issue an outside-of-district warrant." 809 F.3d at 1113 n. 4 (emphasis added). And here numerous district courts have held the NIT warrant fully complied with Rule 41, while others rejected the validity of the warrant, but nonetheless conceded that it was "tempting to view the NIT as a tracking device" under Rule 41(b)(4). *United States v. Workman*, 205 F. Supp. 3d 1256, 1262 (D. Colo. 2016). At a minimum, it was "genuinely unclear" whether the magistrate had the authority to issue the NIT warrant.

To establish prejudice from a Rule 41 violation, a defendant must show he was "subjected to a search that would not have occurred or would not have been so abrasive

---

11 The defendant correctly points out that the Seventh Circuit cases did not involve a warrant specifically determined to be void *ab initio.* But even a warrant that is void *ab initio* can be saved by the Good Faith Doctrine. *United States v. Dorosheff*, 2017 WL 1532267, * 6 (C.D. IL, April 27, 2017) ("In *United States v. Master*, the Sixth Circuit applied the good faith exception to a warrant issued without authority because it was issued by a retired judge. 614 F.3d 236 (6th Cir. 2010). There the court abrogated its earlier holding . . . that the good faith exception could not apply to a warrant that was void *ab initio.* The *Master* court found that such a rule was 'no longer clearly consistent with current Supreme Court doctrine.' *Master,* 614 F.3d at 242.").

had the rules been followed." *United States v. Burgos-Montes*, 786 F.3d 92, 109 (1st Cir. 2015) (quotations and citation omitted). *See also United States v. Stockheimer,* 807 F.2d 610, 613-14 (7th Cir. 1986). The operative question is whether the search would have occurred had the rules been followed. Given the evident constitutionality of the NIT Warrant, the answer here is yes. The NIT Warrant satisfied the Fourth Amendment's probable cause and particularity requirements and thus, had it been presented to a federal magistrate judge in this district, ("a magistrate judge with authority in the district … has authority to issue a warrant to search for … property located within the district") Rule 41(b)(1) would have authorized the very same search of Savage's computer that occurred. *See Darby*, 190 F. Supp. 3d at 537 (finding no prejudice because Rule 41(b)(1) authorized search of defendant's computer, located in Eastern District of Virginia). *Cf. United States v. Martinez-Zayas*, 857 F.2d 122, 136 (3d Cir. 1988) ("this warrant could have been obtained from a federal magistrate"); *United States v. Ritter*, 752 F.2d 435, 441 (9th Cir. 1985) (declining to suppress evidence because there was "no indication that a federal magistrate would have handled the search differently than did the state judge").

iv. Even if the NIT warrant violated Rule 41(b), law enforcement officers acted in good faith.

A well-trained officer would not have understood that the NIT warrant violated Rule 41(b). When the FBI sought judicial approval for this NIT warrant, it had previously received judicial approval to use similar NITs in other cases. *See, e.g.*, *United States v. Laurita*, No. 8:13CR107, 2016 WL 4179365, *6 (D. Neb. Aug. 5, 2016) (re-

affirming, under Rule 41(b)(4), the use of a NIT originally authorized in 2012); *see also Levin*, *supra* (identifying three unsealed, judicially-authorized NIT warrants issued before 2015). The FBI agents could have reasonably relied on the fact that courts have approved warrants to deploy those other similar NITs.

The affidavit submitted to the magistrate clearly indicated that the NIT would be deployed to "activating computer[s]—wherever located." (R. 13-1, pg. 29, ¶ 46(a)). Thus, there can be no question the FBI anticipated the NIT would find its way to computers outside of the Eastern District of Virginia, and that the magistrate was advised as such. The magistrate judge, aware that the NIT would be deployed in such a manner, could have reasonably concluded that she was authorized under Rule 41(b)(4) to issue a warrant permitting the FBI to use such an investigatory technique. The officers were entitled to rely on that determination. *United States v. Mykytiuk*, 402 F.3d 773, 777 (7th Cir. 2005) (fact that an officer obtained a search warrant is *prima facie* evidence the officer was acting in good faith.).

Further, as addressed *supra*, the magistrate who issued the NIT warrant in this case is hardly the only federal judge to decide that it was wholly valid, and no circuit court has yet addressed the issue. The very fact that federal courts have reached varying legal conclusions on the issue proves that "[r]easonable minds" have differed on the legal sufficiency of the NIT warrant. *United States v. Leon*, 468 U.S. 897, 914 (1984); *cf. Heien v. North Carolina*, 135 S. Ct. 530, 540 (2014) (finding that an officer's erroneous interpretation of an ambiguous "stop lamp" law, which had not previously been construed by state appellate courts, was objectively reasonable). That fact mandates

deference to the magistrate's decision. *Leon*, 468 U.S. at 914. Thus, it was not unreasonable for the FBI agents to have deferred to, and relied on, the magistrate judge's implicit finding that she had territorial authority to issue the NIT warrant.

The defendant points to nothing in the record to support the agents intentionally disregarded Rule 41 in seeking the NIT warrant. Instead, he makes unsupported allegations errors in this case "were systemic, involving actors from the high levels of the Department of Justice down to the agents in the field." (R. 12, pg. 18). But the record establishes the FBI acted with scrupulous regard for the requirements of Rule 41 and the Constitution. Faced with the daunting task of apprehending thousands of individuals who were engaging in horrifying child pornography crimes while cloaked in the anonymity that Tor provides, the FBI deployed a sophisticated NIT to unmask and locate them. FBI agents drafted a detailed warrant affidavit that explained the NIT and its operation, provided the basis for probable cause, and described with particularity the places to be searched and things to be seized. Special Agent Macfarlane then presented the warrant application and affidavit to a neutral and detached magistrate judge in the district with the strongest known connection to the criminal activity under investigation. After Special Agent Macfarlane obtained the facially valid warrant authorizing the use of the NIT, the FBI relied on it and executed the search according to the terms of the warrant. "The FBI agents in this case did the right thing" and "should be applauded for [their] actions." *Darby*, 190 F. Supp. 3d at 538.

Assuming *arguendo* this Court rejects the government's Rule 41(b)(4) argument above, the fact that the warrant was later found defective because of the magistrate

judge's mistaken interpretation of her territorial authority does not render the agents' reliance on the warrant objectively unreasonable. The Supreme Court recently reaffirmed that principle, holding that it is not objectively unreasonable for a police officer to rely on a magistrate judge's mistaken assessment of probable cause. *Strieff*, 136 S. Ct. at 2056. "The FBI's investigation into Playpen involved sophisticated and novel technology—used both by the operators and users of Playpen as well as the federal investigators—and the FBI made a reasonable attempt to structure a search warrant that complied with rules that have not evolved as quickly as the technology." *Allain*, 213 F. Supp. 3d at 252. Such conduct does not warrant the application of the exclusionary rule.

Perhaps most importantly, the absence of any deterrence benefit is underscored by the enactment of Rule 41(b)(6). The amendment authorizes a magistrate judge sitting "where activities related to a crime may have occurred … to issue a warrant to use remote access to search" a computer "located within or outside" the magistrate's district if the location of the computer "has been concealed through technological means." Fed. R. Crim. P. 41(b)(6)(A). The amendment was intended, in part, to address the fact that "child abusers sharing child pornography may use proxy services designed to hide their true IP addresses." Honorable Reena Raggi, Report of the Advisory Committee on Criminal Rules 8 (May 6, 2015), *available at* http://www.uscourts.gov/sites/default/files/2015-05-criminal_rules_report_0.pdf. That is exactly what defendant was attempting to accomplish by accessing Playpen through Tor. Given that Playpen was being hosted in the Eastern District of Virginia, it

is indisputable that the magistrate would have had authority to issue the NIT warrant under Rule 41(b)(6)(A).

The "amendment is evidence that the drafters of the Federal Rules do not believe that there is anything unreasonable about a magistrate issuing this type of warrant; the Rules had simply failed to keep up with technological changes." *Darby*, 190 F. Supp. 3d at 538; *Acevedo-Lemus*, 2016 WL 4208436 at *8 ("It would be strange indeed for the Court to suppress the evidence in this case in the face of a strong signal from the Supreme Court that Rule 41 should explicitly permit the issuance of warrants like the NIT Warrant."). The Supreme Court's order that the amendment "shall govern in all proceedings in criminal cases thereafter commenced and, insofar as just and practicable, all proceedings then pending" emphasizes that point. The amendment also establishes that any "violation of Rule 41 is regrettable but unlikely to recur." *Cazares-Olivas*, 515 F.3d at 730. There is minimal, if any, deterrence benefit to be found in sanctioning law enforcement conduct that the drafters of the Federal Rules, the Supreme Court, and Congress have concluded is entirely appropriate.

The costs of suppression, on the other hand, are significant. The court's order denying suppression, if reversed, would exclude "reliable, trustworthy evidence bearing on [defendant's] guilt or innocence," *Davis*, 564 U.S. at 237, of an abhorrent crime that for decades has been "'a serious national problem.'" *Paroline,* 134 S. Ct. at 1716 (quoting *New York v. Ferber*, 458 U.S. 747, 749 (1982)). The facts of the Playpen investigation and defendant's case make the extent of the problem disturbingly apparent. As detailed above, defendant admitted to accessing Playpen through Tor and

to being one of the more than 150,000 Playpen users. "Considering the unspeakable harm caused by child pornography, and the creative and limited conduct of the FBI that was undertaken to mitigate that harm, th[is] Court [should] ha[ve] no trouble concluding that suppression is entirely unwarranted here." *Acevedo-Lemus*, 2016 WL 4208436 at *8.

4. The search warrant was supported by probable cause.

The defendant's final challenge to the NIT warrant, "Problem #4," makes two separate but related arguments: 1) that the defendant had a reasonable expectation of privacy in the contents of his home computer; and 2) that the search was not supported by probable cause. (R. 12, pg. 18). Both arguments are meritless.

i. Savage had no reasonable expectation of privacy in his IP address.

The most critical piece of information obtained by the NIT warrant - the defendant's IP address - is information that ordinarily would have been publicly available and therefore the defendant cannot claim a reasonable expectation of privacy. *United States v. Caira,* 833 F.3d 803, 806-07 (7th Cir. 2016). *See also United States v. Suing*, 712 F.3d 1209, 1213 (8th Cir. 2013) (defendant "had no expectation of privacy in [the] government's acquisition of his subscriber information, including his IP address and name from third-party service providers"); *United States v. Christie*, 624 F.3d 558, 573-74 (3d Cir. 2010) ("[N]o reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties, including [Internet Service Providers].").

Several courts have found this principle applies in the context of Tor and NITs. *See e.g., Laurita* at *5 ("Even an Internet user who employs the Tor network in an attempt to mask his or her IP address lacks a reasonable expectation of privacy in his or her IP address."); *Matish*, 193 F. Supp. 3d at 615 ("Even an Internet user who employs the Tor network in an attempt to mask his or her IP address lacks a reasonable expectation of privacy in his or her IP address."); *Werdene*, 188 F. Supp. 3d at 444 ("Werdene had no reasonable expectation of privacy in his IP address. Aside from providing the address to Comcast, his internet service provider, a necessary aspect of Tor is the initial transmission of a user's IP address to a third-party: 'in order for a prospective user to use the Tor network they must disclose information, including their IP addresses, to unknown individuals running Tor nodes, so that their communications can be directed toward their destinations.'") (citing *United States v. Farrell*, Case No. 15-CR-029, 2016 WL 705197, at *2 (W.D. Wash. Feb. 23, 2016)); *Michaud*, 2016 WL 337263, at *7 ("Mr. Michaud 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.") (citing *Forrester*, 512 F.3d at 510).

Savage had no expectation of privacy in his IP address, particularly because the IP address only identified the defendant. The actual search of his computers contents was, as discussed above, based solely on his consent. Because Savage had no expectation of privacy in his IP address, a warrant to capture it was not even needed and no further analysis of the warrant need be completed.

ii. The NIT warrant was supported by probable cause.

Notwithstanding the question of whether the defendant had a reasonable expectation of privacy in his IP address, the NIT warrant was supported by probable cause.

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

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

As detailed below, nothing in Savage's Motion to Suppress undermines this conclusion. The defects he identifies, if they are even considered defects, are neither of

constitutional magnitude nor the result of an intention on the part of the FBI to mislead the magistrate or skirt the rules. Savage's contrary assertions find no support in the record. Defendants seeking the extraordinary remedy of suppression must clear a high hurdle. Savage falls far short, and his motion should therefore be denied.

iii. Legal standard for probable cause.

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. "When an affidavit is the only evidence presented to a judge in support of a search warrant, the validity of the warrant rests solely on the strength of the affidavit." *United States v. Peck*, 317 F.3d 754, 755 (7th Cir. 2003).

"A search warrant affidavit establishes probable cause when it 'sets forth facts sufficient to induce a reasonable prudent person to believe that a search thereof will uncover evidence of a crime.'" *United States v. Jones*, 208 F.3d 603, 608 (7th Cir. 2000) (quoting *United States v. McNeese*, 901 F.2d 585, 592 (7th Cir. 1990)). In deciding whether an affidavit establishes probable cause, "courts must use the flexible totality-of-the-circumstances standard set forth in *Illinois v. Gates*, 462 U.S. 213, 238." *McNeese*, 901 F.2d at 592. Applying the totality-of-the circumstances standard, "[t]he task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238.

"[P]robable cause is a fluid concept – turning on the assessment of probabilities in particular factual contexts." *Id*. at 232. Thus, "[i]n dealing with probable cause, . . . as the very name implies, we deal with probabilities. These are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." *Brinegar v. United States*, 338 U.S. 160, 175 (1949).

The court's duty in reviewing a search warrant and its supporting materials is limited to ensuring "that the magistrate had a 'substantial basis for . . . [concluding]' that probable cause existed." *Gates*, 462 U.S. at 238-29 (quoting *Jones v. United States*, 362 U.S. 257, 271 (1960)).

iv. As all other courts have previously determined, the NIT warrant affidavit amply supports the magistrate judge's finding of probable cause for issuance of the NIT warrant.

Savage contends that the NIT warrant was not supported by probable cause. In support, he contends that the website's home page failed to "unabashedly announce" that it was a child pornography website.[12]

Savage's arguments are meritless for several reasons. For instance, his contention that the illicit purpose of Playpen "could not be discerned without obtaining a membership and logging in" (despite images of partially clothed prepubescent girls, the unique registration terms and warnings, the graphic content listing upon registration, etc.) is nothing more than a self-serving, skewed interpretation of the affidavit.

[12] Elsewhere in the motion, Savage contends that omissions in the warrant undercut probable cause. Those contentions are erroneous and are addressed on pages 48-51. However, for purposes of this aspect of his motion, the government will treat Savage's contentions regarding the omissions as true.

Moreover, the affiant's description of the main page was only one of many factors contributing to the probable cause determination. Among other things, the affidavit explained the unique nature of the Playpen site on the Tor network and the numerous affirmative steps required to access the site. Moreover, Savage's arguments regarding the likelihood of a user's login to the site fall flat because, for the myriad reasons described in the affidavit, access by an accidental browser was extremely unlikely.

Savage bases his argument in part on *United States v. Wilder*, 526 F.3d 1 (1st Cir. 2008) the proposition that probable cause cannot be established because Playpen's content wasn't readily apparent and its content and nature couldn't be discerned without obtaining a membership and logging in. However, Savage did far more than "merely access" a website; Savage took all the necessary steps to access Playpen, including downloading specific Tor software to anonymize his IP address, locating the specific Playpen web address, viewing the main page (which contained images of partially clothed prepubescent females with their legs spread as well as other information that created a strong inference that the site contained child pornography), viewing the Playpen registration page (which contained further inferences that the site contained illicit material), creating and registering an account for Playpen, and logging in to that account. Savage attempts to use *Wilder* to limit the Court to look only at the homepage of Playpen for probable cause, rather than the totality of the circumstances. *See Allain*, 213 F. Supp. 3d at 244-45 (differentiating Playpen cases from *Wilder*).

In all, the affiant set forth specific, articulable facts that, along with interferences drawn from his training and experience, established probable cause to believe that

registered users who logged into Playpen did so intending to view and trade child pornography. *See generally, e.g., Gates*, 462 U.S. at 238 (discussing probable cause standard); *United States v. Pritchard,* 745 F.2d 1112, 1120 (7th Cir. 1984) (discussing standard of review on challenge to magistrate judge's finding of probable cause); *United States v. Elst*, 579 F.3d 740, 746 (7th Cir. 2009) ("Experienced law enforcement officers (as well as experienced magistrates) are permitted to draw reasonable inferences from the facts based on their training and experience.").

v. The affidavits alleged omissions do not undercut the affidavit's probable cause.[13]

The first alleged omission Savage complains about is the supposed intentional failure of the NIT warrant to advise the magistrate court about a misconfiguration in the website, which allowed public access to it. (R. 12, 21-22). This argument fails because it simply is not true. The information was part of the NIT warrant and was presented to the magistrate judge. (R. 13-1, pgs. 26-27, n. 7) ("Due to a misconfiguration of the TARGET WEBSITE that existed for an unknown period of time, the true IP Addresses of a small number of users of the TARGET WEBSITE (that amounted to less than 1% of registered users of the TARGET WEBSITE) were captured in the log files stored on the Centrilogic server.").

The second alleged omission Savage complains about is the inaccurate description of the site's logo in the NIT warrant. Savage claims the "logo wasn't suggestive of the website's purpose when including two images, and less so with the

[13] The Court already determined that a *Franks* hearing was not warranted in this case.

number reduced to one." (R. 12, pg. 22). According to him, this was a reckless omission that affected probable cause. (Id.). Savage is wrong on this point for several reasons. First, there is no evidence that any omission of the administrator's change to the Playpen logo just before the NIT warrant was authorized was reckless, let alone intentional. Indeed, the affiant had checked Playpen on February 18, 2015, the day before the logo changed, and the description was accurate at that time. (R. 13-1, pgs. 17-18, ¶¶ 11-12 & n.3). The most that can be said is that, with the benefit of hindsight, it would have been better for the affiant to have reviewed Playpen again the morning the warrant was signed, as opposed to two days before. If this is a failing at all, which is by no means obvious, it was - at worst - an unintentional oversight of an immaterial matter. *See, e.g., Darby*, 190 F. Supp. 3d 533 ("There is nothing reckless about relying on a visit to the website on February 18, 2015 when describing the website for a warrant signed and executed on February 20, 2015."); *Matish*, 193 F. Supp. 3d at 606 ("The Court also finds that it was not reckless for the affiant not to examine the website one more time on the day he sought the warrant's authorization, as he had recently examined the website and confirmed that nothing had changed.").[14]

Moreover, even assuming that failing to include a sentence referencing the changed image was somehow intentional and reckless (though it was not), the image change was utterly immaterial to the finding of probable cause. As noted, the images of two partially clothed prepubescent girls with their legs open were on the website up

[14] The district court in *Matish* took testimony from government agents on this point. Upon consideration of the testimony, which was subject to cross-examination, the court found no support for the defendant's position. *See Matish*, 193 F. Supp. 3d at 598.

until February 19, 2015. The replacement of those two sexually suggestive images of prepubescent girls with one sexually suggestive image of a prepubescent girl the day before the warrant was issued in no way calls into question the illicit nature of the website. The relevance of the image(s) in the Playpen logo was that it/they sexualized young girls. That was true before February 19, 2015, and it remained true after. *See e.g.*, *Darby*, 190 F. Supp. 3d at 531 ("To the extent one can or should differentiate among sexualized depictions of children, the images of the two girls that were previously on the homepage are more reprehensible. But that distinction does not subtract from the sexualized nature of the single image of child erotica that appeared on the homepage during the period in which the government operated Playpen. Either version of the homepage supports a finding of probable cause."); *Matish*, 193 F. Supp. 3d at 606 (finding that "the logo change was not material to the probable cause determination" and citing testimony); *Michaud*, 2016 WL 337263, at *1 n.1 (noting court's oral denial of defendant's motion requesting *Franks* hearing); *United States v. Owens*, No. 16-CR-38-JPS, 2016 WL 7079617, at *6 (E.D. Wis. Dec. 5, 2016) (finding that "even if the affiant had accurately described the homepage, there would have been probable cause for the search."). On top of this, as detailed above, the magistrate judge's probable cause finding rested on a host of facts and inferences that demonstrated a "fair probability" that anyone who logged into Playpen did so intending to view and/or share child pornography. *See Gates*, 462 U.S. at 238–39 (noting that "[t]he task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, . . . there is a fair probability that

contraband or evidence of a crime will be found in a particular place); *see also Darby*, 190 F. Supp. 3d at 534 ("As discussed, contrary to the repeated emphasis of Defendant, the images of two prepubescent females described in the warrant application were not necessary to the finding of probable cause. There was an abundance of other evidence before the magistrate judge that supported her finding that there was probable cause to issue the warrant.").

In summary, officers obtained the evidence in this case from the defendant's valid consent to search his computer. That should end the inquiry into the validity of the warrant. If the Court considers the application of the warrant in this case, the inquiry should still end because the defendant had no expectation of privacy in his IP address. When combined with his consent to search his computer, the warrant does not come into play. Even if the Court considers the validity of the warrant, the defendant's motion should be denied because the NIT warrant was a valid warrant that particularly described the places to be searched, was executed reasonably, and was supported by probable cause.

C. The government's conduct in this case was not outrageous.

Savage argues that the Due Process Clause of the Fifth Amendment requires dismissal of his indictment because, he claims, that the maintenance of the site was outrageous government conduct.

The government's conduct during the investigation was not outrageous, nor even unreasonable. Under Supreme Court jurisprudence, outrageous government behavior that "shocks the conscience" may require a dismissal of an indictment under

the Due Process Clause of either the Fifth or the Fourteenth Amendments. *Rochin v. California*, 342 U.S. 165, 172 (1952) (Fourteenth Amendment); *United States v. Russell*, 411 U.S. 423, 431 (1973) (Fifth Amendment). However, the Seventh Circuit does not recognize outrageous government behavior as a defense. *United States v. Smith*, 792 F.3d 760, 765 (7th Cir. 2015) (noting the Seventh Circuit does not recognize an "outrageous government conduct" defense); *United States v. Stallworth*, 656 F.3d 721, 730 (7th Cir. 2011) ("Outrageous government conduct is not a defense in this circuit."); *United States v. White*, 519 F.3d 342, 346 (7th Cir. 2008) ("[T]his circuit clearly and consistently has refused to recognize any defense based on ... 'outrageous government conduct.' "); *United States v. Childs*, 447 F.3d 541, 545 (7th Cir. 2006) (noting that, while the Supreme Court "has left open the possibility of" granting such relief, the Seventh Circuit has never taken the "extreme step of dismissing criminal charges against a defendant because of government misconduct"); *United States v. Garcia*, 89 F.3d 362, 367 (7th Cir. 1996) (noting that the Seventh Circuit "has expressly refused to recognize the doctrine of 'outrageous governmental conduct.' "); *United States v. Boyd*, 55 F.3d 239, 241 (7th Cir. 1995) (holding that the doctrine of "outrageous government misconduct ... does not exist in this circuit"). In addition, developing case law suggests that today, *Rochin* would be evaluated under the Fourth Amendment rather than the Due Process Clause. *Cty. Of Sacramento v. Lewis*, 523 U.S. 833, 850 n.9 (1998); *see generally Owens*, 2016 WL 7079617 at *4–5.

Even if the Seventh Circuit recognized outrageous government conduct as a reason to dismiss a case, the conduct in this case falls far short of what could possibly be

required. The government's conduct was not even unreasonable, let alone outrageous. The FBI did not create Playpen, nor did it induce the defendant to become a member. It did not post any child pornography or links to child pornography to the site, and it certainly did not inspire in the users a desire to view and download child pornography. Rather, with 24/7 monitoring and having presented its plan to two different federal judges, the FBI seized on a fleeting opportunity to identify and apprehend pedophiles using an anonymous network to conceal their active participation in sexual exploitation of children.

An immediate takedown of the site would have merely shifted the site's traffic to another site. Instead, the government maintained the site for two weeks, far less than the thirty days allowed by the warrant and much less than the months that the site had been active. In doing so, the government effected over three hundred arrests, and over fifty human trafficking have victims have been identified or rescued. Given the difficulty of identifying child pornographers on the Tor network, maintenance of the site was necessary to avoid alerting Playpen's members to the government's investigation.

The behavior of the government in the Playpen investigation was based on experienced and reasonable reactions to the difficulties of investigating child

pornography. Consequently, even if outrageous government conduct were a defense, the dismissal of Savage's indictments would not be warranted.

Dated this 17th day of July 2017.

Respectfully submitted,

JEFFREY M. ANDERSON
Acting United States Attorney

By: /s/

ELIZABETH ALTMAN[15]
Assistant U. S. Attorney

15 University of Wisconsin law student Joe Malone, who is an intern in this office, contributed significantly to this brief.