UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA

v. Case No. 17-CR-11-WMC

BRIAN SAVAGE,
Defendant.

BRIEF IN SUPPORT OF SAVAGE'S MOTION TO EXCLUDE EVIDENCE AND DISMISS THE INDICTMENT

I. To collect the evidence against Savage, the FBI operated the world's largest child pornography website, while its agents injected malware into private computers and committed an untold number of federal felonies.

While the FBI ran Playpen, the world's largest child pornography website, one hundred thousand users logged on a total of one million times.[1] In thirteen days, the FBI's Operation Pacifier distributed a quantity of child pornography that the government can't calculate, while Playpen users posted 43 series of new child pornography and 13,000 links to external sources.[2] The number of images viewed, downloaded and redistributed while the FBI managed the website remains unknown.[3]

---

[1] Government response to order compelling discovery, *United States v. Michaud,* Case No. CR15-5351 (W.D. Wash., Jan. 8, 2016)("*Michaud* discovery response") at 4, App. 10; Transcript, *United States v. Matish*, Case No. 16-CR-16 (E.D. Va. May 19, 2016) ("*Matish*") at 50, App. 8.

[2] *Michaud* discovery response at 3, App. 10; Discovery memorandum, *United States v. Tippens,* Case No. 16-5110RJB (Oct. 28, 2016)("*Tippens* discovery memo") at 5, App. 11.

[3] *Michaud* discovery response at 2-4, App. 10.

The FBI took over Playpen on February 20, 2015, purporting to identify its 184,000 users by hacking into their computers.[4] To do so, the agents deployed malware called a "Network Investigative Technique" (NIT) into the "activating computers" of persons logging into the website.[5] The NIT traveled to the activating computer to collect information, including its Media Access Control (MAC) and Internet Protocol (IP) addresses, operating system type, OS user name, and host name.[6] The NIT deployed in a quarter-second without the user's knowledge, then returned the captured information to the FBI's computer, leaving no trace behind.[7]

After taking control of the website, the agents swiftly imported a feature to facilitate distribution of child pornography, Playpen's file-hosting feature, from a server located in Canada.[8] The FBI learned of its location on February 20 and notified Canadian authorities, who shut down the server and sent a copy of the feature to the FBI.[9] Agents installed the file-hosting feature on a government computer in Virginia

---

[4] *Michaud* discovery response at 2-3, App. 10; Transcript, *United States v. Jean*, Case No. 15-CR-50087 (W.D. Ark. June 23, 2016)("*Jean*") at 39-40, App. 5 (NIT works similarly to techniques used by unethical hackers).

[5] Warrant application, Case No. 15-SW-89 (E.D. Va. Feb. 20, 2015)("NIT warrant"), Attachment A, App. 1; *United States v. Jean*, 207 F. Supp. 3d 920, 927 (W.D. Ark. Sept. 13, 2016)(NIT amounts to malware).

[6] NIT warrant, Attachment B, App. 1; Transcript, motion to compel hearing, *United States v. Kneitel,* Case No. 16-CR-23 (M.D. Fla. Nov. 9, 2016)("*Kneitel* compel") at 136, App. 6; Transcript, *United States v. Kneitel,* Case No. 16-CR-23 (M.D. Fla. Dec. 12, 2016)("*Kneitel*") at 142, App. 7.

[7] *Jean* at 46, 86, App. 5; *Kneitel* compel at 148, App. 6.

[8] Transcript, *United States v. Anzalone,* Case No. 15-10347 (D. Mass. Oct. 14, 2016) ("*Anzalone*") at 50-56, App. 3. File hosting allowed users to upload larger files, generally encrypted archives that contained either multiple images or larger videos, without causing the Playpen website to run more slowly. *Anzalone* at 25-26, 55, App. 3.

[9] *Anzalone* at 50-51, App. 3.

and announced its resumption the following day.[10] Users soon reported improved performance, although Daniel Alfin, Pacifier's primary case agent, said the FBI made no upgrades to the website.[11]

Alfin began monitoring Playpen after the website came on-line in August 2014.[12] Playpen operated as a "hidden service" on the TOR network and could be accessed through links available at sources such as TOR index websites.[13] Because TOR masks its users' Internet Protocol addresses, Alfin couldn't determine the IP address of Playpen's server, information that could yield its location.[14]

Foreign authorities provided Playpen's IP address to Alfin in December 2014 and notified him that, due to a configuration error, the website could be accessed on the regular internet.[15] Alfin used the IP address to locate the Playpen server in Lenoir, North Carolina, by December 23.[16] The FBI seized a copy of the website's data from that server on January 15, 2015, without interrupting Playpen's operation.[17]

---

[10] *Anzalone* at 55, App. 3; *Playpen forum posts* at 1, App. 12.

[11] *Playpen forum posts* at 6-16, App. 12; *Anzalone* at 7, 16-17, App. 3. Whether the capabilities of the FBI server in Newington, VA, were greater than the server hosting Playpen in Lenoir, North Carolina is not known. Discovery of this information will be requested.

[12] *Anzalone* at 20-21, App. 3.

[13] *Jean* at 19-20, App. 5

[14] *Matish* at 44-45, App. 8; *Jean* at 32-33, App. 5. *See also* www.torproject.org.

[15] *Anzalone* at 23, App. 3; *Kneitel* at 124, App. 7; Application and order for interception of electronic communications, Case No. 15-ES-4 (E.D. Va.)("wiretap warrant") at ¶38, Dkt. 14. This passage was partially redacted in the wiretap warrant provided in discovery. App. 2. An unredacted copy is filed as Dkt. 14, under seal at the government's request.

The foreign agency likely was the National High Tech Crime Unit of the Netherlands National Police Services Agency, which alerted the FBI to the existence of a child pornography website called PedoBook in 2011, resulting in an investigation dubbed Operation Torpedo. Warrant, Case No. 12-MJ-356 (D. Neb.)("Torpedo warrant") at ¶¶19-25, App. 13.

[16] *Anzalone* at 21, 26-27, App. 3; wiretap warrant at ¶38, Dkt. 14.

[17] *Anzalone* at 24-27, App. 3.

The agents could have shut Playpen down right then, but instead permitted the website to continue running on the North Carolina server.[18] Protocols were discussed to address ethical issues of allowing Playpen's continued operation, but Alfin knew of none that were formulated.[19] By the time the agents began to operate Playpen over a month later, file-hosting and image hosting features had been added to facilitate users' posting child pornography content.[20]

While fifty thousand users accessed Playpen every week, FBI agents discussed taking over the website with lawyers from "Main Justice": the DOJ sections for Child Exploitation and Obscenity, and Computer Crime and Intellectual Property.[21] The FBI's General Counsel and Operational Technology Division were consulted; Agent Douglas Macfarlane believed General Counsel was "intimately involved" because "they work very closely with our unit to review operations exactly such as this."[22]

"Higher up" FBI and DOJ executives made the decision to apply for a warrant to utilize the NIT.[23] Alfin contributed a significant amount to the warrant affidavit, which senior Main Justice attorneys reviewed.[24] The warrant's cover sheet specified the Eastern District of Virginia; Attachment A, its description of the places to be searched, stated the NIT would deploy on the government computer in that district.[25] The actual

---

[18] *Anzalone* at 30-31, App. 3.

[19] *Anzalone* at 47, 57, App. 3.

[20] *Kneitel* at 103-04, App. 7

[21] *Anzalone* at 10, 42-45, App. 3.

[22] *Anzalone* at 46, App. 3; Transcript, *United States v. McLamb,* Case No. 16-CR-92 (E.D. Va. Nov. 1, 2016)("*McLamb*") at 13-14, App. 9.

[23] *Anzalone* at 45-46, App. 3.

[24] *Kneitel* compel at 31, App. 6; *McLamb* at 9, App. 9.

[25] NIT warrant at 1 & Attachment A, App. 1. *See also* Torpedo warrant at 1, App. 13; Transcript, *United States v. Gaver,* Case No. 16-CR-88 (S.D. Ohio, Jan. 17, 2017)("*Gaver*") at 59-65, App. 4 (cover sheet of Torpedo warrant specified "the District of Nebraska and elsewhere.")

places to be searched were computers of persons who logged into Playpen.[26]

A local AUSA and a Main Justice lawyer accompanied Agent Macfarlane to submit the warrant application to U.S. Magistrate Judge Theresa Carroll Buchanan.[27] At the time, Fed. R. Crim. P. 41 didn't authorize the magistrate judge to approve warrants for NIT searches conducted outside her district, although a district court judge could do so.[28] Earlier that day, an agent obtained an order from a district court judge in the same courthouse authorizing interception of Playpen users' communications.[29]

After Magistrate Judge Buchanan signed the warrant, the FBI began deploying the NIT from the Playpen website installed on their computer in Virginia, unguided by any written operational plan.[30] Although the warrant specified deployment at log-in by any activating computer, the agents configured the NIT to deploy after a user logged in and accessed a post on specified sub-forums.[31] The agents set the NIT to deploy at log-in for administrators and moderators, described by Alfin as "the high level ranking people . . . responsible for running the criminal enterprise."[32] But the NIT failed to deploy

---

[26] *Matish* at 61, App. 8.

[27] *Michaud* discovery response at 8, App. 10

[28] Rule 41 was amended to allow magistrate judges to issue NIT warrants effective December 1, 2016. *See also United States v. Krueger*, 809 F.3d 1109, 1125 & n.6 (10th Cir. Kan. 2015)(Rule 41 doesn't preclude extra-district warrants issued by district court judges).

[29] *Jean* at 81-82, App. 5; Wiretap warrant, Dkt. 14.

[30] *Kneitel* at 121, App. 7. The agents generated no reports of analysis of data obtained after seizing a copy of the website, when they identified members, administrators and moderators, *Kneitel* at 102, App. 7; of meetings with programmers to craft the NIT, *Kneitel* compel at 72, App. 6; describing the operational plan to deploy the NIT, *Kneitel* at 121, App. 7; documenting successful deployment of the NIT, *Kneitel* compel at 116, App. 6; or notifying the issuing judge of efforts to minimize harm to victims. *Kneitel* compel at 154, App. 6.

[31] NIT warrant, Attachment A, App. 1; *Anzalone* at 62, App. 3.

[32] *Jean* at 46, 85-86, App. 5; *Kneitel* compel at 66, App. 6. After the first few hours, the agents began deploying the NIT only when they knew it would be successful. *Kneitel* at 144-49, App. 5. How success could be determined pre-deployment, according to Alfin, is classified. *Id.*

against any administrator or moderator because, as Alfin explained, "[t]heir computers did not appear to be susceptible to the technology we used."[33]

Playpen averaged over three thousand log-ins per hour while the FBI ran the website from February 20 to March 4, 2015. Of 100,000 user accounts meeting the warrant's conditions for deploying the NIT, the FBI collected 8,713 IP addresses, of which 1,332 were located in the United States.[34] On May 1, 2017, the DOJ reported domestic arrests of 350 persons.[35] One was Brian Savage.[36]

II. Because the government violated the Warrant and Reasonableness Clauses of the Fourth Amendment in seizing information from Savage's computer, all evidence obtained or derived from that search must be suppressed.

Agent Macfarlane probably felt optimistic when he arrived at the courthouse to swear out the affidavit for the Playpen warrant. Macfarlane wasn't assigned to Operation Pacifier, hadn't done any investigative work on the case, and didn't possess Alfin's technical knowledge.[37] But senior DOJ attorneys reviewed the affidavit, two government lawyers accompanied him, and Judge Trenga had approved the wiretap warrant first thing that morning. Only Magistrate Judge Buchanan's signature separated the FBI from operating the largest child pornography website in the world.

Macfarlane and the DOJ lawyers might have foreseen problems with the NIT warrant. Because evident problems existed.

---

[33] *Kneitel* at 120, App. 7.

[34] *Jean* at 64-65, App. 5; *Tippens* discovery memo at 2-3, App. 11.

[35] https://www.justice.gov/opa/pr/florida-man-sentenced-prison-engaging-child-exploitation-enterprise (visited June 10, 2017).

[36] Additional facts appear in the argument section of this brief.

[37] *Kneitel* at 132, App. 7; *Kneitel* compel at 30-31, 142, App. 6.

A. Problem #1: The warrant failed to particularly describe the places to be searched and granted impermissible discretion to the agents.

The NIT warrant 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. That's unconstitutional. The Fourth Amendment's Warrant Clause requires particular identification of the places to be searched, leaving nothing to the discretion of the agents.

Neither the warrant nor its affidavit stated the agents' intention to deploy the NIT to search 50,000 computers located worldwide--each week, for thirty days.[38] The warrant's cover page stated the property to be seized would be located in the Eastern District of Virginia. Attachment A, its description of the places to be searched, described "the use of a network investigative technique (NIT) to be deployed on the computer server . . . located at a government facility in the Eastern District of Virginia."[39]

Macfarlane knew the NIT's operation couldn't be restricted to the Eastern District of Virginia.[40] He believed the NIT warrant's description of the targeted suspects as "any user or administrator" conveyed that information.[41] He also believed its affidavit conveyed that the agents sought leave to search computers located anywhere

---

[38] NIT warrant, App. 1; *Anzalone* at 10, App. 3. The NIT warrant, at ¶19, App. 1, stated that 11,000 users accessed Playpen each week.

[39] NIT warrant, Attachment A, App. 1: "This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below. The computer server is the server operating the Tor Network child pornography website referred herein as the TARGET WEBSITE . . . which will be located at a government facility in the Eastern District of Virginia. The activating computers are those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password."

[40] *McLamb* at 6-7, App. 9; *Matish* at 32-33, 62-65, App. 8.

[41] NIT warrant, Attachment A, App. 1; *McLamb* at 33-34, App. 9; *Gaver* at 62, 67-68, App. 4.

in the world.[42]

The affidavit doesn't communicate that fact with its single reference in its forty-sixth paragraph to "an activating computer–wherever located."[43] The same paragraph also advised that repeated searches of activating computers might be performed.[44] In footnote 8, the affidavit mentioned the possibility that the agents might deploy the NIT "more discretely against particular users."[45]

But the agents couldn't permissibly rely on passages buried in the affidavit to broaden the warrant's geographic scope or narrow the places to be searched. First, the affidavit wasn't incorporated by reference into the NIT warrant. *See United States v. Stefonek*, 179 F.3d 1030, 1033 (7th Cir. 1999). Next, a broad-ranging affidavit can't expand the express limitations imposed by the magistrate in issuing the warrant itself. *United States v. Sedaghaty*, 728 F.3d 885, 913 (9th Cir. 2013). The description in the warrant, not the language of the affidavit, determines the places to be searched. *Stefonek, supra*; *Sedaghaty*, 728 F.2d at 914.

The NIT warrant also didn't authorize multiple searches of individual computers, although Alfin believed the agents could deploy the NIT "as many times as

---

[42] *Gaver* at 57.

[43] The affidavit's only other reference to the warrant's geographic scope refers to "an activating computer–wherever located." NIT warrant at ¶46, App. 1.

[44] NIT warrant at ¶¶44, 46, App. 1.

[45] NIT warrant at ¶ 32, n. 8, App. 1 ("in executing the requested warrant, the FBI may deploy the NIT more discretely against particular users, such as those who have attained a higher status on Website 1 by engaging in substantial posting activity, or in particular areas of TARGET WEBSITE, such as the TARGET WEBSITE sub-forums described in Paragraph 27.")

In contrast, the Torpedo warrant's attachment describing the places to be searched specified the NIT would be activated by users accessing any page in PedoBook's images section or who sent or viewed private messages. Torpedo warrant, Attachment A, App. 1.

we wanted to against any user of the website."[46] One warrant generally authorizes one search. *See United States v. Keszthelyi*, 308 F.3d 557, 568-569 (6th Cir. 2002). A second entry may be made as a continuation of the original search, *id.*, but successive deployment of the NIT isn't a continuation. Repeated hacking into a private computer differs significantly from returning to the scene of a search with a mechanic to open the hood of a bank robber's car. *See United States v. Gerber*, 994 F.2d 1556, 1559 (11th Cir. 1993).

The warrant didn't authorize "discrete deployment," either. But the agents exercised almost unlimited discretion, capturing 8,713 IP addresses from 100,000 log-ins that met the warrant's requirement for deploying the NIT.[47] The agents could have sought a warrant to search the computers of specific website users and the FBI ostensibly possessed the technology needed to do so.[48] Instead, the agents obtained a warrant they knew would authorize searching 50,000 computers each week, then decided to search nine percent of them.

That's constitutionally prohibited. A lawful warrant can't authorize searches of numerous places and leave to the agents' discretion which places should be searched and how many times to search them. That's far too close to the operation of a writ of assistance: specifying the object of a search and leaving which places should be searched to the discretion of the police. *Steagald v. United States*, 451 U.S. 204, 220 (1981).

The particularity requirement's central purpose is to restrict the discretion exercised by government agents. *Berger v. New York*, 388 U.S. 41, 98–99 (1967). It protects against open-ended warrants that leave the scope of the search to the discretion

---

[46] *Kneitel* at 120, App. 7.

[47] *Tippens* discovery memo at 3, App. 11; *Jean* at 65, App. 5.

[48] *Matish* at 69-70, App. 8; NIT warrant at ¶¶19, 32 n. 8, App. 1.

of the officer. *United States v. Clark*, 754 F.3d 401, 410 (7th Cir. 2014) citing *Stanford v. Texas*, 379 U.S. 476, 485–86 (1965). A warrant satisfies the particularity requirement if it leaves nothing about its scope to the discretion of the officer serving it. *Clark, supra,* citing *Jones v. Wilhelm*, 425 F.3d 455, 462 (7th Cir.2005).

Because the NIT warrant failed to specify the places to be searched with particularity and granted impermissible discretion, the NIT warrant is void, unconstitutional and facially invalid. *Massachusetts v. Sheppard*, 468 U.S. 981, 988 n. 5 (1984)*; Groh v. Ramirez*, 540 U.S. 551, 557 (2004); *Jacobs v. City of Chicago,* 215 F.3d 758, 767 (7th Cir. 2000) citing *Horton v. California*, 496 U.S. 128, 139–40 (1990). Given that the particularity requirement is set forth in the text of the Constitution, no reasonable officer could believe that a warrant that plainly did not comply with that requirement was valid. *Groh,* 540 U.S. at 563. On these facts, objective good faith is absent. *See*; *United States v. Leon*, 468 U.S. 897, 923 (1984); *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 325 (1979).

Lack of particularity and impermissible discretion void the NIT warrant. Good faith doesn't salvage the fruit of its poisonous tree. The evidence against Brian Savage derived from the search of his computer must be suppressed.

B. Problem #2: The execution of the NIT warrant victimized the children portrayed in Playpen's content, violating the Fourth Amendment's Reasonableness Clause.

For thirteen days, the government continually committed every crime alleged by the NIT warrant affidavit: possession, receipt, advertisement and distribution of child pornography, and engaging in a child exploitation enterprise.[49] That list doesn't

[49] NIT warrant at ¶4, App. 1 (listing 18 U.S.C. §§2251(d)(1) and (e), 2252A(a)(2) and (b)(1), 2252A(a)(5)(B) and (b)(2), and 2252A(g)).

encompass the agents' countless violations of 18 U.S.C. §3509(m) by releasing child pornography from government custody and innumerable international laws.[50]

Advised by DOJ lawyers, the FBI agents committed an exponentially greater number of crimes than did the persons reportedly arrested. Those persons, other than the website's administrators, largely appear to have been, like Savage, retail consumers of child pornography who readily confessed when confronted by police.[51] The FBI's wholesale distribution of an incalculable quantity of child pornography dwarfs their offenses.

But the government most egregiously violated the Reasonableness Clause by re-victimizing the children portrayed in the website's content.

The DOJ lawyers and FBI agents certainly foresaw that Operation Pacifier would distribute an immense quantity of child pornography. They undoubtedly understood that every viewing of every image distributed by the FBI would cause "a repetition of the victim's abuse." *Paroline v. United States*, 134 S. Ct. 1710, 1727 (2014). As the Justice Department reported to Congress, "The child victims are . . . victimized again when these images of their sexual assault are traded over the Internet in massive numbers by

---

[50] In Operation Pacifier, 84% of the IP addresses captured by the NIT were located in 120 countries outside the United States. *Tippens* discovery memo at 3, App. 11. International law prohibits the government from undertaking law enforcement functions without those countries' consent. *See U.S. Attorney's Criminal Resource Manual* at § 267. No record indicates that the government sought any foreign sovereign's aid or consent before deploying the NIT malware on computers located abroad. In contrast, Netherlands authorities notified the United States and other countries before commencing its NHTCU investigation. Torpedo warrant at ¶19, App. 13.

[51] A search of 55 Playpen decisions available on Lexis, performed June 11, 2017, found that 26 defendants confessed when confronted. One decision stated the defendant falsely denied misconduct and 28 decisions didn't divulge whether the defendant cooperated.

like-minded people across the globe."[52]

The absence of effort to mitigate that re-victimization emphasizes the government's hypocrisy and cruelty. In other investigations, the FBI deployed the NIT upon activation of links with explicit titles where only an error message would appear.[53] Investigators reportedly use "spoofing" to secretly redirect website visitors to a sanitized facsimile of the site, or utilize child erotica or "virtual" child pornography to avoid tipping off suspects.

But other than deleting a very small amount of content, the FBI kept the entire Playpen website available.[54] The FBI didn't delete or disable any links to external sources, although capable of doing so.[55] The agents shut down Producer's Pen, a little-used sub-forum for producers of child pornography, but that didn't affect users' ability to post, view and redistribute new and pre-existing content.[56]

The Fourth Amendment's Reasonableness Clause requires that agents conduct a search in a reasonable manner. *See United States v. Ramirez*, 523 U.S. 65, 71 (1998). Fourth Amendment reasonableness controls both the manner and scope of executing of a warrant. *See United States v. Ganias*, 824 F.3d 199, 209 & n.21 (2d Cir. 2016). The manner in which a warrant is executed is subject to later judicial review as to its reasonableness. *Dalia v. United States*, 441 U.S. 238, 258 (1979).

---

[52] DOJ, *Report to Congress: The National Strategy for Child Exploitation Prevention and Interdiction* at 3 (Aug. 2010); https://www.justice.gov/psc/docs/natstrategyreport.pdf (visited June 10, 2017).

[53] *See* "FBI Admits It Controlled Servers Behind Mass Malware Attack," Wired, September 13, 2013, at https://www.wired.com/2013/09/freedom-hosting-fbi/ (visited June 10, 2016)(FBI-controlled hidden service sites displayed "down for maintenance" message).

[54] *Kneitel* at 112, App. 7; *Kneitel* compel at 120-21, App. 6.

[55] *Kneitel* compel at 57-58, App. 6

[56] *Anzalone* at 19-20, 56, App. 3; *Kneitel* compel at 95-96, App. 6.

Determining whether police action is reasonable under the Fourth Amendment requires an objective analysis of the facts known to the police at the time of the action. *Brigham City v. Stuart*, 547 U.S. 398, 404 (2006). Those facts include agents' knowledge that 50,000 users would access child pornography on Playpen 500,000 times each week that the FBI ran the website.[57] Given the Court's statement in *Paroline* and DOJ's lip service to that principle, the government's decision to perpetuate that victimization can't be characterized as reasonable.

Courts have warned that official conduct far less expansive than the Playpen warrant's execution is unacceptable. In *United States v. Sherman,* 268 F.3d 539 (7th Cir. 2001), the Court criticized investigators' delivery of one child pornography photo set and one videotape to Sherman's home.

> [T]he government's participation in criminal activity in the course of an investigation should rarely, if ever, involve harming actual, innocent victims. . . . Moreover, the government's dissemination of the pornographic materials to Sherman could hardly be described as a "controlled" delivery of the materials. Given the length of time that Sherman was allowed to possess these materials before he was arrested, the government's conduct here could easily have led to further victimization of the children depicted because the defendant had an opportunity to copy the materials and disseminate them to others.
>
> *Sherman*, 268 F.3d at 549.

In Pacifier, the government repudiated every concern expressed in *Sherman*. The FBI didn't use two items for bait, then retrieve both. The Bureau distributed an unknown number of images, re-victimizing actual, innocent victims countless times while ignoring the DOJ's own investigative principle, "[b]ecause digital information can be easily copied and communicated, it is difficult to control distribution in an online

---

[57] *Anzalone* at 10, App. 3.

operation and so limit the harm that may arise from the operation."[58] The FBI didn't conduct a controlled delivery; Pacifier's distribution of child pornography went out of their control at its outset, as the agents knew it would.

The reasonableness of executing a warrant balances the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion. *See Graham v. Connor*, 490 U.S. 386, 396 (1989). Savage's privacy expectations are self-evident, and further discussed below. The government's interest in enforcing the laws against possession and dissemination of child pornography is equally apparent.

The government disregarded that interest in distributing countless immortal images of child pornography worldwide, so this Court should give it no weight. Further, assertion of the agents' good faith is irrelevant and inapplicable to situations where the manner of execution of a warrant is challenged. *United States v. Husband*, 226 F.3d 626, 636 n. 6 (7th Cir. 2000) quoting LaFave, *Search and Seizure*, § 1.3(f) (3d ed. 1996).

This Court should denounce and deter the government's execution of the NIT warrant, which insouciantly dismissed as a cost of doing business the distribution of a mind-blowing quantity of child pornography. Because the agents unreasonably executed the NIT warrant, the Fourth Amendment's Reasonableness Clause requires that this Court order suppression of all evidence gained through or derived from its execution.

---

[58] DOJ, *Online Investigative Principles for Federal Law Enforcement Agents* at 44 (1999), available at .https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf (visited June 10, 2017).

C. Problem #3: The NIT affidavit failed to communicate its worldwide scope to the magistrate judge who approved it, resulting in a warrant void ab initio.

After serving eighteen years as a U.S. Magistrate, Judge Buchanan undoubtedly understood the Rule 41(b) limits on her authority to issue warrants for searches outside her district.[59] Review of the facts and preceding events illustrates that she approved the NIT warrant, which clearly exceeded those limits, after being misled as to its scope and manner of execution.

1. While the DOJ sought amendment of Rule 41 to permit magistrate judges' approval of NIT warrants, Playpen fell into the FBI's lap.

During 2012, the FBI conducted a smaller-scale NIT investigation called Operation Torpedo. Defendants raised Rule 41 issues in the Torpedo cases, all venued in Nebraska, but any violations were held nonprejudicial. *See, e.g., United States v. Welch,* 811 F.3d 275 (8th Cir. 2016).

In the year separating the Torpedo and Pacifier operations, a magistrate judge ruled that a NIT warrant exceeded the territorial limits of Rule 41 and failed to satisfy the requirement of particularity. *In re Warrant to Search a Target Computer at Premises Unknown,* 958 F.Supp. 2d 753, 756-60 (S.D. Texas April 22, 2013). Later in 2013, the DOJ recommended to the Advisory Committee on Criminal Rules that Rule 41 be amended to permit magistrate judges' approval of NIT warrants, and submitted a follow-up memo dated December 22, 2014.[60] The next day, Alfin located the Playpen server in

---

[59] Judge Buchanan became a U.S. Magistrate during September 1996. *See* https://www.bloomberg.com/profiles/people/3898045-theresa-carroll-buchanan (visited June 10, 2017). The Federal Magistrate's Act, 28 U.S.C. §636(a), also did not supply authority for a magistrate judge to issue a search outside of the district.

[60] *See* Raman Rule 41 letter, Sept. 18, 2013, App. 14; DOJ Memorandum, Dec. 22, 2014, App. 15.

North Carolina, presenting the Justice Department with an ideal scenario for use of a NIT warrant.

The high-level Main Justice lawyers directing the Pacifier operation surely knew that Magistrate Judge Buchanan couldn't authorize searches outside of her district. The intention to hide the ball from her explains why a warrant reviewed by senior DOJ attorneys lacks clear and accurate description of the places to be searched. The senior DOJ attorneys ostensibly approved burial by footnote of the affidavit's content about agents discretely narrowing the searches. That information belonged in Attachment A, as did the provision for multiple searches that was relegated to the affidavit's forty-fourth paragraph.

On the same day, in the same courthouse, an FBI agent submitted the Pacifier wiretap warrant application to a district court judge. Another judge asked later why the NIT warrant wasn't submitted to Judge Trenga, who had gained familiarity with Pacifier by reviewing the wiretap warrant. Alfin answered that application to the magistrate judge "could have been done as a normal course of business."[61] He might have added that submission to Judge Trenga, being a deviation from the normal course of business, could have raised hard-to-answer questions.

2. Rule 41's tracking device provision didn't encompass the NIT, which searched the activating computers rather than tracking their location.

The DOJ lawyers undoubtedly convinced Magistrate Judge Buchanan that Rule 41's tracking device provisions supplied her authority to approve the NIT warrant. They'd convinced MacFarlane that the NIT functioned as a tracking device, although he

[61] *Jean* at 82-83, App. 5.

conceded that it remotely searched computers.[62] The government's tracking device theory is superficially appealing but completely wrong-headed. Rule 41(b)(4) authorizes tracking devices, not the installation of a device that searches for information that it then sends back to the government.[63]

The facts illustrate that the warrant's vague, disjointed description misled the magistrate judge about the scope and operation of the NIT's deployment. Magistrate Judge Buchanan approved the warrant because she believed the DOJ lawyers' assertion that the NIT is a tracking device, which it isn't, and wouldn't search outside the district, which it did. No other reason appears to explain why a magistrate judge with her experience would approve the NIT warrant.

3. The NIT warrant was void ab initio with respect to Savage because it authorized searches outside the jurisdiction of the issuing judge.

But Magistrate Judge Buchanan wasn't authorized to issue a warrant with worldwide, or even Wisconsin-wide, application. A warrant for a search outside the jurisdiction of the issuing judge is void ab initio. *See United States v. Master*, 614 F.3d 236, 239 (6th Cir. 2010)*; United States v. Krueger*, 809 F.3d 1109, 1115-17 (10th Cir. 2015)(Gorsuch, J., concurring)*; Bishop Paiute Tribe v. Cty. of Inyo*, 291 F.3d 549, 568 (9th Cir. 2002), vacated on other grounds, 538 U.S. 701. Although the Seventh Circuit held that violations of federal rules do not justify exclusion of evidence seized on the basis of

---

[62] *Gaver* at 67-68, App. 4; *Matish* at 61, 65, App. 8. Alfin analogized the NIT to "an Internet aged [sic] tracker." *Kneitel* at 156, App. 7.

[63] *United States v. Broy*, 209 F. Supp. 3d 1045, 1056 (C.D. Ill. 2016); *see also* 18 U.S.C. § 3117 ("the term "tracking device" means an electronic or mechanical device which permits the tracking of the movement of a person or object.")

On May 12, 2017, a Lexis search revealed 35 decisions finding Rule 41(b)(4) inapplicable to the Playpen NIT warrant.

probable cause, *United States v. Cazares-Olivas*, 515 F.3d 726, 730 (7th Cir. 2008), that case did not involve a warrant specifically determined to be void ab initio. *United States v. Broy*, 209 F. Supp. 3d 1045, 1057 (C.D. Ill. 2016).

Exclusion is the correct disposition because the facts of Savage's case present more than a rules violation. Submission of the NIT warrant to a magistrate judge wasn't just business as usual. Credulity can't withstand the strain of suggestion that DOJ personnel unknowingly or unthinkingly submitted the NIT warrant application to a judge lacking jurisdictional authority. Additional key facts, discussed below, were concealed to ensure she approved it.

On this record, there should be no question of good faith.[64] The warrant procurement process created an error that played a causal role in the seizure and stemmed from disdain of the constitutional requirements for searching a home computer. *See Cazares-Olivas*, 515 F.3d at 728. This error was systemic, involving actors from high levels of the Department of Justice down to the agents in the field. Despite the subsequent amendment of Rule 41, the deterrence of exclusion isn't marginal. *See Herring v. United States*, 555 U.S. 135, 147 (2009). A message can be sent about the importance of integrity to the system.

D. Problem #4. Savage had a reasonable expectation of privacy in the contents of his home computer and its search wasn't supported by probable cause, particularly when omitted facts are considered pursuant to *Franks v. Delaware*.

1. By understating the likelihood of an innocent or inadvertent visit to the website, the warrant affidavit failed to supply probable cause.

[64] Four district courts, dealing with identical facts, held that the good faith exception doesn't apply when police execute a void ab initio warrant. *United States v. Croghan*, 209 F. Supp. 3d 1080 (S.D. Iowa 2016); *United States v. Workman*, 205 F. Supp. 3d 1256 (D. Colo. 2016); *United States v. Arterbury*, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67092 (N.D. Okla. May 17, 2016); *United States v. Levin*, 186 F. Supp. 3d 26 (D. Mass. 2016).

Savage enjoyed a reasonable privacy expectation in the location where the NIT searched, his home computer. *See United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004); *Broy*, 209 F.Supp.3d at 1054, *see also* 18 U.S.C. § 1030(a)(2)(C)(prohibiting hacking). For that reason, the NIT's extraction of information from Savage's computer was a Fourth Amendment search, requiring a warrant supported by probable cause.

Alfin believed that probable cause of criminality existed once a person logged on to Playpen by entering a user name and password.[65] That may be true if the website's home page "unabashedly announced that its essential purpose was to trade child pornography." *United States v. Martin*, 426 F.3d 68, 75 (2d Cir. 2005). Because Playpen's home page didn't convey that message at all, merely logging into the website failed to provide probable cause to deploy the NIT to search the activating computer.

A website's home page met the "unabashed announcement" standard by presenting images of nude and partially-dressed girls, some prepubescent, along with this text: "Lolitagurls.com offers hard to find pics! With weekly updates and high quality pix inside, you cant go wrong if you like young girls!" *United States v. Gourde*, 440 F.3d 1065,1067 (9th Cir. 2006) (en banc).[66] The homepage for Lust Gallery displayed thumbnail images featuring unclothed minors and promised "A Secret Lolitas Archive" where "[a]ll models inside are 14 or younger." *United States v. Wilder*, 526 F.3d 1, 9-10 (1st Cir. 2008).

Playpen's home page didn't describe the site's content and its nature couldn't be discerned without obtaining a membership and logging in. The page most prominently

---

[65] *Jean* at 38, App. 5.

[66] Other websites satisfied the test by offering lengthy descriptions of their content prior to log-in. *See Martin, supra; United States v. Froman*, 355 F.3d 882, 890-91 (5th Cir. 2004); *United States v. Shields*, 458 F.3d 269, 271 (3d Cir. Pa. 2006).

advertised the existence of Playpen chat.[67] The Playpen logo appeared, initially two girls and, at the time of the FBI takeover, one girl.[68] None of those images were child pornography or even overtly suggestive, and the images were very small.[69] Alfin failed to notice the logo change when he viewed the revised web page on February 19, and he'd been monitoring Playpen for months.[70]

Because Alfin didn't observe the change, the NIT warrant affidavit failed to advise Judge Buchanan of it. That's a critical omission because the warrant sought to establish probable cause by minimizing the possibility of inadvertent access.[71] The NIT warrant affidavit emphasized the steps required to access Playpen--use of the TOR browser and acquisition of the site's TOR address--and unequivocally stated, "A user may only access the TARGET WEBSITE through the TOR network."[72]

That's not true. Alfin knew by December 2014 that Playpen could be accessed and its true IP address discerned through the regular internet. The FBI didn't correct the configuration error that permitted regular internet access, so Playpen remained accessible without using the TOR browser until the agents shut down the website months later.[73] Alfin never checked to find out whether Playpen could be located by

---

[67] *See* Playpen Logo 2, App. 17.

[68] *See United States v. Michaud*, 2016 U.S. Dist. LEXIS 11033, *8 (W.D. Wash. Jan. 28, 2016)("While the warrant application for the NIT describes a main page featuring two prepubescent females with legs spread apart, at ¶12, by the time that the FBI submitted the warrant application, on February 20, 2015, the main page had been changed to display only one young female with legs together.")

[69] *See* Playpen logo 1, App. 16; Playpen Logo 2, App. 17.

[70] *Jean* at 34-35, App. 5.

[71] NIT warrant at ¶¶ 7-10, App. 1.

[72] NIT warrant at ¶10, App. 1.

[73] *Anzalone* at 33-34, App. 3.

using a regular internet search engine.[74]

Given Playpen's unrevealing home page and the affidavit's inaccuracies, merely logging on to the site with a user name and password "does not remotely satisfy Fourth Amendment standards." *See United States v. Corea,* 419 F.3d 151, 156 (2d Cir. 2005). Basing probable cause on a user's mere log-in tracks an erroneous argument that probable cause exists to search a person based on propinquity to others independently suspected of criminal activity. *Corea, id.,* quoting *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979). The NIT warrant overbroadly based probable cause on mere presence, due to its affidavit's understatement of the likelihood of an inadvertent user's log-in to the site.

2. Analysis of misrepresentations and omissions under *Franks v. Delaware* emphasizes the absence of probable cause to search Savage's computer.

The wiretap warrant stated, "Due to a misconfiguration of the server hosting the TARGET WEBSITE, the TARGET WEBSITE was available for access on the regular internet to users who knew the true IP address of the server. After receiving the tip from the foreign law enforcement agency, an FBI agent, acting in an undercover capacity, accessed IP address 192.198.81.106 and resolved to the TARGET WEBSITE."[75]

That passage appeared in the first paragraph of a section entitled "Identification and Seizure of the Computer Server Hosting the TARGET WEBSITE." The NIT warrant omitted it from an identically-worded paragraph in its identically-entitled section.[76]

---

[74] *Jean* at 70-71, App. 5. It's not known whether Playpen's actual URL (uniform resource locator) became visible when viewed on the regular internet.

[75] Wiretap warrant at ¶38, Dkt. 14.

[76] NIT warrant at ¶28, App. 1.That paragraph concluded with a sentence, not included in the wiretap warrant, "Further investigation has identified a resident of Naples, FL, as the suspected administrator of the TARGET WEBSITE, who has administrative control over the computer server in Lenoir, NC, that hosts the TARGET WEBSITE."

Instead, the NIT warrant unequivocally stated that Playpen couldn't be accessed on the regular internet.[77]

The absence of one key sentence from an otherwise identical section can't be attributed to accident. The omission of information from the NIT warrant about accessing Playpen by the regular internet appears intentional.

A second omission appears reckless. Alfin reviewed the web page on the day before the NIT warrant was submitted, but failed to observe that its logo had changed. The logo wasn't suggestive of the website's purpose when including two images, and less so with the number reduced to one. Alfin knew the content of the affidavit and the importance of the website's first page to its presentation of probable cause. But the affidavit wasn't corrected to notify Magistrate Judge Buchanan of that critical change.

Evidence seized under a warrant must be suppressed when the defendant shows that the affidavit in support of the warrant contains misleading omissions, the omissions were made deliberately or with reckless disregard for the truth, and probable cause would not have existed without the omissions. *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978); *United States v. Featherly*, 846 F.3d 237, 239–40 (7th Cir. 2017).

Inclusion of these omissions deducts two foundational blocks from the affidavit's probable cause showing. Incidences of inadvertent visitors become increasingly possible, directly decreasing the paltry quantum of probable cause to insufficiency. On these facts, good faith cannot apply, because Judge Buchanan was misled by the agents' omission of information from the NIT warrant, either made deliberately or with reckless disregard of the truth. *Leon*, 468 U.S. at 897, citing *Franks, supra.*

---

[77] NIT warrant at ¶10, App. 1. ("A user may only access the TARGET WEBSITE through the Tor network.")

III. Problem #5: The government's outrageous conduct in re-victimizing the children portrayed by the website's content warrants dismissal.

Child pornography is so repulsive a crime that those entrusted to root it out may, in their zeal, be tempted to bend or even break the rules. *United States v. Coreas*, 419 F.3d 151 (2d Cir. 2005). The rules bent and broken by the government in Operation Pacifier illustrate the outrageousness of its conduct in this case.

The FBI agents and DOJ lawyers over-reached by submitting an unparticularized warrant supported by attachments that concealed the warrant's scope. Their affidavit omitted facts that emphasize the lack of probable cause to invade Savage's privacy expectations by deploying malware to search his computer. They weren't forthright with Judge Buchanan about the manner and scope of the NIT's deployment, inducing a violation of Rule 41 and producing a warrant void ab initio.

But most outrageous by far is the incredible hypocrisy and callous cruelty to the victims displayed by the conduct of the FBI agents and DOJ lawyers. While committing countless crimes, the government re-victimized every child portrayed in the innumerable images that the FBI distributed, in order to make 350 arrests.

Alfin said no protocols were formulated for dealing with ethical issues of the government's operation of Playpen, but he was wrong. Operation Pacifier was guided by a protocol stating that the end justified the means.

But the DOJ's own pronouncements, and those of the Courts in *Paroline* and *Sherman*, establish that the end of a few hundred arrests doesn't justify harming any number of innocent victims. That means-end justification does not and should not exist in American criminal justice:

> To declare that in the administration of the criminal law the end justifies the means — to declare that the government may commit crimes in order to secure the conviction of a private criminal — would bring terrible retribution. Against that pernicious doctrine this court should resolutely set its face.

Olmstead v. United States, 277 U.S. 438, 485 (1928), Brandeis, J., dissenting.

Savage requests this Court order dismissal of the indictment that charges him, based on the government's conduct in the Playpen investigation. He understands that circuit precedent does not recognize the defense of outrageous government conduct. *United States v. Boyd*, 55 F.3d 239, 241 (7th Cir.1995). However, Supreme Court and other Court of Appeals authority confirm that defense exists. *United States v. Russell*, 411 U.S. 423, 431 (1973); *United States v. Black*, 733 F.3d 294, 298 (9th Cir. 2013).

The government's conduct in procuring the Playpen warrant will not astonish those familiar with the often competitive enterprise of ferreting out crime. But the conscience should be shocked by the staggering volume and global scope of the government's distribution of pornographic images, each one a re-victimization of the child portrayed.

Russell predicted that a court may someday be presented with a situation in which the conduct of law enforcement agents is so outrageous that due process principles absolutely bar the government from invoking judicial processes to obtain a conviction.

That day is today.

Respectfully submitted this 14th day of June, 2017.

MEYER LAW OFFICE
Attorney for Brian Savage

/s/ Stephen J. Meyer
Stephen J. Meyer
SBN: 1011807

Address:
10 E. Doty St. Ste. 800
Madison, WI 53703
608-255-0911
defender6@aol.com

CERTIFICATION OF SERVICE

I certify that I have served the above document on the office of the United States Attorney by CM/ECF.

/s/ Stephen J. Meyer
Stephen J. Meyer