United States v. Ammons

United States District Court for the Western District of Kentucky, Louisville Division

September 14, 2016, Decided

CRIMINAL ACTION NO. 3:16-CR-00011-TBR-DW

Reporter
2016 U.S. Dist. LEXIS 124503

UNITED STATES OF AMERICA, Plaintiff, v. DENNIS AMMONS, Defendant.

Core Terms

magistrate judge, users, suppression, good-faith, website, network, federal magistrate, circumstances, Internet, seized, expectation of privacy, child pornography, exclusionary rule, accessed, hidden, server, holds, search warrant, no authority, void, law-enforcement, deterrence, warrantless search, ab initio, computer's, deliberate, searched, exigent

Opinion

[*1] MEMORANDUM OPINION AND ORDER

Dennis Ammons has been indicted for knowingly producing and receiving child pornography. His prosecution originates from the Government's investigation of "Playpen," a website dedicated to the distribution and discussion of matters pertinent to child pornography and the sexual abuse of children. Though a website, Playpen could not be accessed through the traditional Internet. Instead, Playpen existed on "The Onion Router" network (or "Tor," for short). The Tor network conceals the internet protocol addresses of its users, thereby thwarting traditional techniques employed to identify Internet users. To circumvent Tor's protections, the Federal Bureau of Investigation obtained a warrant from Magistrate Judge Buchanan of the Eastern District of Virginia to deploy a network investigative technique on Playpen's server. The NIT would instruct a user's computer to transmit certain information-such as the computer's IP address-to the FBI after the user logged on to Playpen. Using the NIT, the FBI identified Ammons as a registered user on Playpen. The FBI obtained a warrant to search his residence located in Muldraugh, Kentucky on the basis of that information. Now, **[*2]** Ammons seeks to suppress all information seized pursuant to the NIT warrant, including the evidence obtained during or as a result of the search of his home.

1

The Court holds that use of the NIT was a "search" within the meaning of the *Fourth Amendment*. Though Magistrate Judge Buchanan issued the NIT warrant, she lacked authority to do so under the *Federal Magistrates Act*, *28 U.S.C. §§ 631-639*, and *Federal Rule of Criminal Procedure 41(b)*. The ensuing search of Ammons' computer, therefore, violated the *Fourth Amendment*. Yet, under the good-faith exception to the exclusionary rule, suppression is not an appropriate remedy for that unconstitutional search. Accordingly, Dennis Ammons' Motion to Suppress, [R. 24], is **DENIED**.

I.

A.

The prosecution of Dennis Ammons originates from the Government's investigation of "Playpen," a website "dedicated to the advertisement and distribution of child pornography" and "the discussion of matters pertinent to child sexual abuse." [R. 24-2 at 14, ¶ 6 (Special Agent Macfarlane's Affidavit).] Though a website, Playpen could not be accessed through the traditional Internet. [*Id.* at 16, ¶ 10.] Instead, Playpen existed on "The Onion Router" network (or "Tor," for short). [*Id.* at 14, ¶ 7.] Tor is designed "specifically to facilitate anonymous communication over the Internet." [R. 24-5 at 17, ¶ 17 (Special **[*3]** Agent MacHenry's Affidavit).] It accomplishes that task in two ways.

First, Tor thwarts traditional techniques employed to identify Internet users. [R. 24-2 at 27-28, ¶ 31.] For example, the Government typically identifies users by obtaining and tracing a computer's internet protocol address. [*See* R. 24-5 at 23, ¶ 32.] Whenever a person accesses a website through the Internet, the website typically logs that computer's IP address. [R. 24-2 at 15, ¶ 8.] If the Government were to seize control of

2

that website, then it could retrieve the logs and discover which IP addresses accessed the site. [R. 24-5 at 23, ¶ 32.] By cross-referencing an IP address with publically-available databases, which list the IP address ranges assigned to various internet service providers, the Government could determine which ISP owned the target IP address. [*Id.*] The Government could then ascertain the identity of the user through an administrative subpoena issued to the ISP. [*Id.*]

Tor changes all of that. Tor masks a user's IP address by routing communications through "a distributed network of relay computers run by volunteers all over the world." [R. 24-2 at 15, ¶ 8.] When a user on the Tor network accesses **[*4]** a website, the only IP address revealed to the site is that of the last computer in the relay, dubbed an "exit node." [*Id.*] It is impossible, though, to trace that IP address back to the originating computer. [*Id.*] Consequently, a user on the Tor network remains effectively anonymous to the websites he or she visits. [*Id.*]

Second, Tor affords anonymity to those who host websites as "hidden services" on the Tor network too. [*Id.* at 15-16, ¶ 9.] A hidden service functions just like any other website with a single exception: The website's IP address is hidden and replaced with a Tor-based address consisting of a series of alphanumeric characters followed by the suffix ".onion." [*Id.*] There is no way to determine the IP address of the server hosting a hidden service. [*Id.*]

A hidden service may only be accessed through the Tor network. [*Id.* at 16, ¶ 10.] Even after connecting to the Tor network, though, a user cannot stumble across a hidden service while using an ordinary search engine, such as Google. [*See id.* at 16-17, ¶ 10.]

3

Instead, a user must know the exact Tor-based address of the hidden service. [*Id.* at 16, ¶ 10.]

Playpen operated on the Tor network as a hidden service from around August 2014 to March 2015. [*Id.* at 16-17, ¶¶ 10-11.] Upon registering **[*5]** for an account, potential users were warned not to enter a real e-mail address or to post identifying information in their profiles. [*Id.* at 18, ¶ 13.] Playpen informed potential users that the website and its administrators were unable to determine the IP addresses of any users' computer. [*Id.* at 18-19, ¶ 13.] In less than one year, more than two-hundred thousand members created and viewed tens of thousands of postings related to child pornography. [R. 24-5 at 19, ¶ 22; *see also* R. 24-2 at 22, ¶ 19.] Images and videos shared through the site were extensively categorized according to the child's age and gender, as well as the type of sexual activity involved. [*See* R. 24-2 at 19-21, ¶ 14.]

In December 2014, a foreign law-enforcement agency advised the Federal Bureau of Investigation

that a United States-based IP address appeared to be associated with Playpen. [*Id.* at 25, ¶ 28.] Shortly after, the FBI confirmed that the IP address belonged to Centrilogic, a server hosting company headquartered in Lenoir, North Carolina. [*Id.* at 25-26, ¶ 28.] The FBI subsequently obtained and executed a search warrant in January 2015. [*Id.*] Upon discovering that the target server contained a copy of Playpen, the FBI transported it to a government-controlled server in **[*6]** Newington, Virginia, located in the Eastern District of Virginia. [*See id.* at 25-27, ¶¶ 28, 30.] On February 19, 2015, the FBI apprehended the suspected administrator of, and assumed control over, Playpen. [*Id.* at 26-27, ¶ 30.]

4

The FBI wished to continue operating Playpen for a limited time (from February 20 to March 5, 2015) so as to identify its users. [*Id.*] To that end, the Government sought and obtained a warrant from Magistrate Judge Buchanan of the Eastern District of Virginia to deploy a network investigative technique (or "NIT," for short) on Playpen's server. [*Id.* at 27-28, ¶ 31; *see also id.* at 2-4 (NIT Search Warrant).] The NIT is a series of code that instructed a user's computer to transmit certain information to the FBI after the user logged on to Playpen. [*Id.* at 28, ¶¶ 32-33.] In detail, the information consisted of the computer's IP address, operating system, "host name," active operating system username, media access control address, and a unique identifier (to distinguish the data sent from other devices). [*Id.* at 4.]

Using the NIT, the FBI determined that a person going by the username "H8RL3Y" had registered on Playpen on March 4, 2015. [R. 24-5 at 24, ¶ 37.] Between March 4 and March 5, "H8RL3Y" accessed several images of **[*7]** child pornography over a six-hour period of activity. [*Id.* at 24-25, ¶¶ 37-39.] Cross-referencing the IP address associated with "H8RL3Y" against publically-available databases, the FBI determined that the IP address belonged to a Time Warner Cable subscriber. [*Id.* at 26, ¶ 40.] Through an administrative subpoena issued to TWC, the FBI traced the IP address to a home in Muldraugh, Kentucky, where Dennis Ammons (along with his sister and her two minor children, "Jane Doe" and "Jane Roe") resided. [*See id.* at 26-27, ¶¶ 41-43; R. 1 at 5-6, ¶¶ 9-11 (Criminal Complaint and Affidavit).]

On December 8, 2015, FBI Special Agent Virginia MacHenry sought and obtained from Magistrate Judge Lindsay in the Western District of Kentucky a warrant to search Ammons' residence for evidence of child pornography. [R. 24-6 at 1 (Residential

5

Search Warrant).] Law-enforcement officers executed that warrant on December 15. [R. 1 at 5, ¶ 9.] During an interview with law-enforcement officers, Ammons admitted to looking at child pornography, but officers made no arrest at that time. [*Id.*]

Subsequently, on December 29, 2015, a staff member with the Family and Children's Place in Louisville, Kentucky, conducted an interview with "Jane Doe," a sixteen-year-old **[*8]** girl. [*Id.* at 6, ¶ 10.] (Special Agent MacHenry observed the interview via closed-circuit television. [*Id.*]) During that interview, Doe recounted an incident where Ammons made her pose fully nude in the "spread-eagle" position on his bed while he photographed her with his cell phone. [*Id.*, ¶ 11.] Doe also described multiple occasions when Ammons forced her to completely undress and sit on his bed "with her legs open while facing Ammons and his computer." [*Id.*, ¶ 12.]

B.

On December 31, 2015, Special Agent MacHenry filed a criminal complaint and affidavit of probable cause, [*see* R. 1 at 1-7], and obtained from Magistrate Judge Brennenstuhl in the Western District of Kentucky a warrant to arrest Ammons, [*see* R. 6 at 1 (Arrest Warrant)]. Law-enforcement

officers arrested Ammons on January 5, 2016. [*Id.*] On February 2, Ammons was indicted for knowingly producing and receiving child pornography. [R. 9 at 1-2 (Indictment).] Now, Ammons seeks to suppress all information seized pursuant to the NIT warrant, including the evidence obtained during or as a result of the search of his home.1 [*See* R. 24 at 1-2 (Motion to Suppress).] Both Ammons and the Government agree that an evidentiary hearing is unnecessary. [*See* R. 32 at 1 **[*9]** (Order of August 1, 2016).]

1Absent the information seized pursuant to the NIT warrant, there is no dispute that the Government would have lacked the probable cause necessary to obtain the residential search warrant.

6

II.

Ammons argument goes something like this: Magistrate Judge Buchanan lacked jurisdiction under the *Federal Magistrates Act*, which incorporates *Federal Rule of Criminal Procedure 41(b)*, to issue the NIT warrant. [R. 24 at 5-7.] In the absence of such jurisdiction, the NIT warrant was void from the beginning. [*Id.* at 7.] Consequently, the Government's search of his computer violated the *Fourth Amendment*. The Government, for its part, resists Ammons on each point. [*See* R. 29 at 2-9 (Response).] In the alternative, the Government finds the good-faith exception to the exclusionary rule applicable in these circumstances. [*Id.* at 13-15.]

The Court holds that use of the NIT was a "search" within the meaning of the *Fourth Amendment*. Though Magistrate Judge Buchanan issued the NIT warrant, she lacked authority to do so under the *Federal Magistrates Act* and *Federal Rule of Criminal Procedure 41(b)*. The ensuing search of Ammons' computer, therefore, violated the *Fourth Amendment*. Yet, Magistrate Judge Buchanan's mistaken belief as to the extent of her jurisdiction, absent any indication of reckless conduct on the Government's part, does not warrant suppression.

III.

A.

The **[*10]** threshold question is whether use of the NIT on Ammons' personal computer was a search under the *Fourth Amendment*. *See Kyllo v. United States, 533 U.S. 27, 31 (2001)* (describing "whether or not a *Fourth Amendment* 'search' has occurred" as the "antecedent question" in such cases). "The *Fourth Amendment* protects '[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable

7

searches and seizures.'" *United States v. Carpenter, 819 F.3d 880, 886 (6th Cir. 2016)* (quoting *U.S. Const. amend. IV*). For purposes of the *Fourth Amendment*, a "search" occurs whenever the Government either "invades an individual's reasonable expectation of privacy" in the place or thing to be searched, *United States v. Anderson-Bagshaw, 509 F. App'x 396, 402 (6th Cir. 2012)* (citing *Smith v. Maryland, 442 U.S. 735, 739-40 (1979)*), or physically intrudes on "a constitutionally protected area," *United States v. Bah, 794 F.3d 617, 630 (6th Cir.)*,*cert. denied sub nom. Harvey v. United States*, ---

U.S. ----, 136 S. Ct. 561 (2015). To demonstrate a search of the first kind, a person must exhibit an actual and subjective expectation of privacy in the thing to be searched or seized that society is prepared to accept as objectively reasonable. *United States v. Mathis, 738 F.3d 719, 729 (6th Cir. 2013)*.

Here, the Court holds that use of the NIT on Ammons' computer was a search within the meaning of the *Fourth Amendment*. *United States v. Adams*, No. 6:16-cr-11-Orl-40GJK, 2016 WL 4212079, at *3-4 (M.D. Fla. Aug. 10, 2016); *United States v. Darby*, --- F. Supp. 3d ----, ----, 2016 WL 3189703, at *4-6 (E.D. Va. 2016).*Contra United States v. Henderson*, No. 15-cr-00565-WHO-1, 2016 WL 4549108, at *5 (N.D.Cal. Sept. 1, 2016);

United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *4-6 (C.D. Cal. Aug. 8, 2016); *United States v. Matish*, --- F. Supp. 3d

----, ----, 2016 WL 3545776, at *18-24 (E.D. Va. 2016); *United States v. Werdene*, --

- F. Supp. 3d ----, ----, 2016 WL 3002376, at *8-10 (E.D. Pa. 2016). There appears to be no dispute that Ammons enjoyed a subjective expectation of privacy in the contents of his personal computer. His expectation was **[*11]** reasonable too. *See United States v. Conner, 521 F. App'x 493, 497 (6th Cir. 2013)* ("Generally speaking, computer users

8

have a reasonable expectation of privacy in data stored on a home computer." (citing

Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001)));*accord United States v. Heckenkamp,482 F.3d 1142, 1146 (9th Cir. 2007)*; *United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004)*; *Trulock v. Freeh, 275 F.3d 391, 402-04 (4th Cir. 2001)*; *Palmieri v. United States, 72 F. Supp. 3d 191, 210 (D.D.C. 2014)*, *appeal dismissed*, No. 14-5289 (D.C. Cir. May 6, 2015). By surreptitiously reprogramming Ammons' computer, the Government intruded on that expectation of privacy. *Darby*, --- F. Supp. 3d at ----, 2016 WL 3189703, at *6; *United States v. Arterbury, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091, at *30 (N.D. Okla. Apr. 25, 2016)*, *adopted by No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67092 (N.D. Okla. May 17, 2016)*. The Court concludes that use of the NIT on Ammons' computer was a *Fourth Amendment* search.

The Government replies, though somewhat perfunctorily, that use of the NIT was not a "search" because Ammons lacked a reasonable expectation of privacy in the information seized, such as in his IP address. [*See* R. 29 at 12.] It is true that, as a general proposition, an individual does not possess a reasonable expectation in his IP address. *See Carpenter, 819 F.3d at 887*; *accord United States v. Christie, 624 F.3d 558, 573-74 (3d Cir. 2010)*; *United States v. Perrine, 518 F.3d 1196, 1204-05 (10th Cir. 2008)*; *United States v. Forrester, 512 F.3d 500, 509-11 (9th Cir. 2007)*. In this case, though, the Government obtained Ammons' IP address from a search of his personal computer-not, for example, from a third-party service provider. *Cf. Carpenter, 819 F.3d at 888* ("Whether a defendant had a legitimate expectation of privacy in certain information depends in part on what the government did to get it."). The Government elides the fact that the NIT warrant describes Ammons' computer as the thing to be

9

searched. [*See* R. 24-2 **[*12]** at 3.] Accordingly, the pertinent inquiry is whether Ammons had a reasonable expectation of privacy in the contents of his personal computer-not merely in his IP address. *See Darby*, --- F. Supp. 3d at ----, 2016 WL 3189703, at *4-5. The Government's argument misses the mark.

B.

Since use of the NIT amounted to a *Fourth Amendment* search, the Court turns to whether the *Federal Magistrates Act*, *28 U.S.C. §§ 631-639*, authorized Magistrate Judge Buchanan to issue the NIT warrant. Under the *Federal Magistrates Act*, a magistrate judge possesses "all powers and duties conferred or imposed . . . by law or by the [Federal] Rules of Criminal Procedure." *28 U.S.C. § 636(a)(1)*. *Federal Rule of Criminal Procedure 41(b)*, in turn, grants magistrate judges the authority to issue warrants in certain circumstances. *See Fed. R. Crim. P. 41(b)(1)-(5)*. *Rule 41(b)(1)* articulates the general principle: A magistrate judge "has authority to issue a warrant to search for and seize a person or property located within the district" of his or her commission. *Fed. R. Crim. P. 41(b)(1)*. There are, of course, exceptions to that general statement. For example, a magistrate judge has authority to issue a warrant for "a person or property outside the district if the person or

property is located within the district when the warrant is issued," *Fed. R. Crim. P. 41(b)(2)*, and for the installation of a tracking device within the district, even if the person or property happens to travel outside the district **[*13]** later, *Fed. R. Crim. P. 41(b)(4)*.

In this case, Ammons argues that Magistrate Judge Buchanan lacked jurisdiction to issue the NIT warrant under *28 U.S.C. § 636(a)*, which incorporates *Federal Rule of Criminal Procedure 41(b)*, because the warrant authorized a search of property located outside (and never inside) her judicial district. [R. 24 at 6-7.] The Government

10

disagrees, maintaining that *Rule 41(b)(1)*, *(2)*, and *(4)* conferred the necessary authority to Magistrate Judge Buchanan. [R. 29 at 6-9.] The Government's position, however, is untenable: The Court holds that Magistrate Judge Buchanan had no authority to issue the NIT warrant under *28 U.S.C. § 636(a)(1)* and *Federal Rule of Criminal Procedure 41(b)*.

1.

Magistrate Judge Buchanan had no authority to issue the NIT warrant under *Rule 41(b)(1)*. *Henderson*, 2016 WL 4549108, at *3; *Adams*, 2016 WL 4212079, at *5;

Darby, --- F. Supp. 3d at ----, 2016 WL 3189703, at *12 n.7;*Werdene*, --- F. Supp.3d at ----, 2016 WL 3002376, at *5-7; *United States v. Levin*, --- F. Supp. 3d ----, --

--, 2016 WL 2596010, at *5-6 (D. Mass. 2016); *Arterbury, 2016 U.S. Dist. LEXIS 67091, at *19*; *United States v. Michaud*, No. 3:15-cr-05351-RJB, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016). *Rule 41(b)(1)* authorizes a magistrate judge "to issue a warrant to search for and seize a person or property located within the district" of his or her commission. *Fed. R. Crim. P. 41(b)(1)*. In this case, the NIT warrant targeted Ammons' computer in the Western District of Kentucky-not in the Eastern District of Virginia. The property to be seized pursuant to the NIT warrant was not the server located in the Eastern District of Virginia, but the IP address and related material from any activating computer that accessed Playpen. *Werdene*, --- F. Supp. 3d at ----, 2016 WL 3002376, at *7. Since that material was located outside the Eastern District **[*14]** of Virginia, Magistrate Judge Buchanan had no authority to issue the NIT warrant under *Rule 41(b)(1)*.

The Government responds that where, as here, it is impossible to identify the location of the property to be searched prior to obtaining a warrant, *Rule 41(b)(1)* ought

11

to be interpreted to allow a magistrate judge "in the district with the strongest known connection to the search" to issue a warrant. [R. 29 at 8-9.] To accept the Government's position, however, the Court would need to add words (and a significant number of them at that) to *Rule 41(b)(1)*. It declines to do so. *See 62 Cases, More or Less, Each Containing Six Jars of Jam v. United States, 340 U.S. 593, 596 (1951)* ("Congressexpresses its purpose by words. It is for us to ascertain-neither to add nor to subtract, neither to delete nor to distort.").

2.

For almost identical reasons, *Rule 41(b)(2)* bestowed no authority on Magistrate Judge Buchanan to issue the NIT warrant. *Henderson*, 2016 WL 4549108, at *3;

Werdene, --- F. Supp. 3d at ----, 2016 WL 3002376, at *7;*Levin*, --- F. Supp. 3d at ----, 2016 WL 2596010, at *6; *Arterbury, 2016 U.S. Dist. LEXIS 67091, at *19-21*;

Michaud, 2016 WL 337263, at *6. *Rule 41(b)(2)* allows a magistrate judge "to issue awarrant for a person or property outside the district if the person or property is located within the district when the warrant is issued." *Fed. R. Crim. P. 41(b)(2)*. The Government suggests that because the NIT was located on its servers in the Eastern District of

Virginia when the warrant issued, *Rule 41(b)(2)* controls. [R. 29 at 8.] Yet, as discussed before, the property to be searched pursuant **[*15]** to the NIT warrant was Ammons' computer in the Western District of Kentucky. His computer was not in the Eastern District of Virginia when the NIT warrant issued. Consequently, *Rule 41(b)(2)* conferred no authority to Magistrate Judge Buchanan to issue the NIT warrant.

12

3.

Rule 41(b)(4) afforded Magistrate Judge Buchanan no authority to issue the NIT warrant either. *Henderson*, 2016 WL 4549108, at *3-4; *Adams*, 2016 WL 4212079, at *6; *Werdene*, --- F. Supp. 3d at ----, 2016 WL 3002376, slip op. at 12-13; *Levin*, ---

F. Supp. 3d at ----, 2016 WL 2596010, at *6; *Arterbury, 2016 U.S. Dist. LEXIS 67091, at *21-22*; *Michaud*, 2016 WL 337263, at *6. *Contra United States v. Laurita*, No. 8:13CR107, 2016 WL 4179365, at *6-7 (D. Neb. Aug. 5, 2016); *Matish*, --- F. Supp. 3d at ----, 2016 WL 3545776, at *17-18; *Darby*, --- F. Supp. 3d at ----, 2016 WL 3189703, at *11-12. Under *Rule 41(b)(4)*, a magistrate judge may "issue a warrant to install within the district a tracking device" on property, even if that property is later transported outside the district. *Fed. R. Crim. P. 41(b)(4)*. Even assuming that the NIT qualifies as a "tracking device," *see* *18 U.S.C. § 3117(b)*; *Fed. R. Crim. P. 41(a)(2)(E)*, the installation occurred not within the Eastern District of Virginia, but in the Western District of Kentucky where Ammons' computer was located. Therefore, Magistrate Judge Buchanan had no authority to issue the NIT warrant under *Rule 41(b)(4)*.

4.

Because Magistrate Judge Buchanan had no jurisdiction or authority under the *Federal Magistrates Act* to issue the NIT warrant, the Court holds that the NIT warrant was void from the beginning (or *ab initio*, in Latin). *See* *United States v. Master, 614 F.3d 236, 239 (6th Cir. 2010)*; *United States v. Peltier, 344 F. Supp. 2d 539, 548 (E.D. Mich. 2004)*; *United States v. Neering, 194 F. Supp. 2d 620, 628 (E.D. Mich. 2002)*. In other words, the warrant on which the Government sought "to justify its search in this

13

case was no warrant at all." *United States v. Krueger, 809 F.3d 1109, 1118 (10th Cir. 2015)* (Gorsuch, **[*16]** J., concurring in the judgment).

C.

The question, then, becomes whether the warrantless search of Ammons' computer violated the *Fourth Amendment*.2 It is axiomatic that a "warrantless search is '*per se* unreasonable under the *Fourth Amendment*-subject only to a few specially established and well-delineated exceptions.'" *United States v. Hudson, 405 F.3d 425, 441 (6th Cir. 2005)* (quoting *Katz v. United States, 389 U.S. 347, 357 (1967)*). One well-recognized "exception applies 'when the exigencies of the situation make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the *Fourth Amendment*." *Kentucky v. King, 563 U.S. 452, 460 (2011)* (alteration in original) (quoting *Mincey v. Arizona, 437 U.S. 385, 394 (1978)*). The Government must shoulder the burden of demonstrating such extraordinary circumstances existed. *United States v. Purcell, 526 F.3d 953, 960 (6th Cir. 2006)*.

Here, the Government points to the "ongoing abuse" of children, as well as the need to obtain users' identifying information, as sufficient justification for conducting the search. [R. 29 at 11-12.] Notwithstanding the weight of those interests, the Court finds no exigent circumstances warranted the search of Ammons' computer. The exigent circumstances doctrine addresses "situations where 'real immediate and serious

2 Although, so far, most courts seem to analyze the

lack of authority to issue the NIT warrant through the lens of a *Federal Rule of Criminal Procedure 41(b)* violation, the Court finds that framework **[*17]** to be inappropriate. Instead, the Court is persuaded by Judge Gorsuch's concurrence in *United States v. Krueger, 809 F.3d 1109 (10th Cir. 2015)*. The error of a *Rule 41* violation is special: It involves "aviolation of the magistrate judge's statutory territorial jurisdiction under *§ 636(a)* as prescribed by Congress," which is "the very sort of jurisdictional limitation on the execution of warrants that the common law and *Fourth Amendment* have enforced since time out of mind." *Id. at 1126 n.7* (Gorsuch, J., concurring in the judgment). Accordingly, the Court looks to whether the there is any justification for a warrantless search of Ammons' computer, as the NIT warrant is simply "no warrant at all." *Id. at 1118*.

14

consequences will certainly occur if a police officer postpones action to obtain a warrant.'" *United States v. Williams, 354 F.3d 497, 503 (6th Cir. 2003)* (quoting *Ewolskiv. City of Brunswick, 287 F.3d 492, 501 (6th Cir. 2002)*). In this case, though, theGovernment not only obtained a warrant,3but continued to operate Playpen for some two weeks. Those facts belie any claim of exigency. *See Darby*, --- F. Supp. 3d at ----,

2016 WL 3189703, at *13 n.8; *cf. United States v. Plavcak, 411 F.3d 655, 664-65 (6th Cir. 2005)* (finding exigent circumstances where confidential informant told agents that suspects were burning documents in anticipation of search). Accordingly, the Court holds that the warrantless search of Ammons' computer was unreasonable and violated the *Fourth Amendment*.

D.

Nonetheless, the Court must decide if suppression is the appropriate **[*18]** remedy for that unconstitutional search. *See United States v. Buford, 632 F.3d 264, 275-76 (6th Cir. 2011)*. Generally speaking, the exclusionary rule "forbids the use of improperly obtained evidence at trial." *Herring v. United States, 555 U.S. 135, 140 (2009)* (citing *Weeks v. United States, 232 U.S. 383, 398 (1914)*). It is "a judicial innovation,"*United States v. Clariot, 655 F.3d 550, 553 (6th Cir. 2011)*, designed to discourage the police fromviolating the *Fourth Amendment*, *Davis v. United States, 564 U.S. 229, 237 (2011)*. Suppression, then, is not "an automatic consequence of a *Fourth Amendment* violation."

Herring, 555 U.S. at 137. Instead, in order for the exclusionary rule to take root, "the

3 The Government seems to suggest that "if the [NIT] warrant could not have been issued, then no warrant could have been obtained in a reasonable amount of time to identify" Playpen's users. [R. 29 at 12 (Response).] The Government's argument is of no moment. Even if no *magistrate*judge could issue the NIT warrant, there is no reason to question the authority of a *district*judge to do so, since the *Federal Magistrates Act* and *Federal Rule of Criminal Procedure 41(b)* "bear only on the authority of magistrate judges to issue warrants." *United States v. Levin*, --- F. Supp. 3d ----, ----, 2016 WL 2596010, at *9 n.15 (D. Mass. 2016).

15

deterrence benefits of suppression must outweigh its heavy costs." *Davis, 564 U.S. at 237* (citing *Herring, 555 U.S. at 141*; *United States v. Leon, 468 U.S. 897, 910 (1984)*).

The good-faith exception to the exclusionary rule, applied across a large swath of cases, reflects that balance. *See id.* at 238-39 (collecting cases). It recognizes that societal costs tend to outweigh the deterrent value of suppression when "the police act with **[*19]** an objectively 'reasonable good-faith belief' that their conduct is lawful, or when their conduct involves only simple, 'isolated' negligence." *Id. at 238* (quoting *Leon, 468 U.S. at 909*; *Herring, 555 U.S. at 137*). In those circumstances, the "'deterrence rationale loses

much of its force,' and exclusion cannot 'pay its way.'" *Id.* (quoting *Leon, 468 U.S. at 907 n.6, 919*). Alternatively, if law-enforcement officers "exhibit 'deliberate,' 'reckless,' or 'grossly negligent' disregard for *Fourth Amendment* rights," then deterrence holds greater value and often outweighs the attendant costs. *Id.* (quoting

Herring, 555 U.S. at 144). The crucial finding "needed to suppress evidence is whetherpolice [mis]conduct [is] sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Master, 614 F.3d at 243* (alterations in original) (quoting *Herring, 555 U.S. at 144*).

In this case, the Government suggests that suppression is inappropriate because the FBI agents reasonably and in good faith obtained, relied upon, and executed the NIT warrant. [R. 29 at 13-15.] Ammons objects. He argues that the good-faith exception is categorically unavailable in situations where a warrant (such as the NIT warrant here) is void *ab initio*. [R. 24 at 9-13.] Even if the good-faith exception **[*20]** were available, though, he maintains the FBI agents could not reasonably rely on the NIT warrant due to the

16

obvious jurisdictional defect. [*Id.* at 13-14.] Though not without some support, the Court finds Ammons' position unpersuasive: Resort to the good-faith exception is not only available, but also is appropriate, in these circumstances.

1.

The Court holds that the good-faith exception is not foreclosed where the warrant relied upon is void *ab initio*. *United States v. Eure*, No. 2:16cr43, 2016 WL 4059663, at *8 (E.D. Va. July 28, 2016); *Werdene*, --- F. Supp. 3d at ----, 2016 WL 3002376, at *11-14. *Contra Levin*, --- F. Supp. 3d at ----, 2016 WL 2596010, at *10-12;

*Arterbury, 2016 U.S. Dist. LEXIS 67091, at *34-38*.

Though the factual circumstancesin this case might differ from those in *Leon*, its rationale applies with equal force. The legal status of a warrant under the *Fourth Amendment* does not, as a categorical matter, limit the reach of the good-faith exception.

The Sixth Circuit Court of Appeals' decision in *United States v. Master, 614 F.3d 236 (6th Cir. 2010)*, requires that conclusion. *Master* involved a search warrant issued by a state judge who lacked the authority to do so under state law. *Id. at 239*. The Court of Appeals held that because warrant was void *ab initio*, the ensuing search violated the *Fourth Amendment*. *Id. at 239-41*. Nonetheless, the good-faith exception still applied, the Court of Appeals reasoned, *id. at 241-43*, and, therefore, remanded the case for findings on "whether [the] 'police [mis]conduct [was] sufficiently deliberate that exclusion **[*21]** [could] meaningfully deter it, and sufficiently culpable that such deterrence [was] worth the price paid by the justice system,'" *id. at 243* (second alteration in original) (quoting *Herring, 555 U.S. at 144*). On remand, the district court denied the motion to suppress on the basis of the good-faith exception, and the Court of Appeals

17

affirmed in an unpublished opinion. *See United States v. Master, 491 F. App'x 593, 594- 97 (6th Cir. 2012)*.

The holding of *Master* is clear: The good-faith exception to the exclusionary rule is not foreclosed in situations where a warrant is void *ab initio*. *Master, 614 F.3d at 241- 43*. Instead, the legal status of a warrant merely informs, but does not control, the Court's good-faith analysis. Jurisdictional limits placed on magistrate judges, after all, must "be respected," and so the exclusionary rule should be used to deter "intentional attempts to avoid" them. *Id. at 243*. Yet, exclusion remains a "last resort"-not a "first impulse," even if a warrant happens to be void from the beginning. *Hudson v. Michigan, 547 U.S. 586, 591 (2006)*.4

2.

In this case, the Court finds suppression to be inappropriate in light of *Herring* and the good-faith exception. *Henderson*, 2016 WL 4549108, at *6; *Adams*, 2016 WL 4212079, at *7-8; *Acevedo-Lemus*, 2016 WL 4208436, at *8; *Matish*, --- F. Supp. 3d at

----, 2016 WL 3545776, at *25; *Darby*, --- F. Supp. 3d at ----, 2016 WL 3189703, at *13-14; *Werdene*, --- F. Supp. 3d at ----, 2016 WL 3002376, at *14-16; *Michaud*, 2016 WL 337263, at *7. *Contra Levin*, --- F. Supp. 3d at ----, 2016 WL 2596010, at *13; *Arterbury, 2016 U.S. Dist. LEXIS 67091, at *35*. Contrary to Ammons' assertion,

4 Though Ammons cites *United States v. Scott, 260 F.3d 512 (6th Cir. 2001)*, *abrogated by United States v. Master, 614 F.3d 236 (6th Cir. 2010)*,*as recognized in United States v. Beals, 698 F.3d 248, 265(6th Cir. 2012)*, in support of his position, [*see* R. 24 at 10-14 **[*22]** (Motion to Suppress)], his reliance is misplaced. True enough, the Sixth Circuit Court of Appeals held in *Scott* that the good-faith exception did not apply "where a warrant [was] issued by a person lacking the requisite legal authority," in that case, a retired state court judge. *Scott, 260 F.3d at 515*. In *Master*, however, the Court of Appeals reexamined *Scott* and found its holding to be no longer viable in light of the Supreme Court's refinement of theexclusionary rule in *Herring v. United States, 555 U.S. 135 (2009)*, and *Hudson v. Michigan, 547 U.S. 586 (2006)*. *See Master, 614 F.3d at 241-43*. Consequently, the Court declines to follow *Scott*'s categorical approach. *United States v. Werdene*, --- F. Supp. 3d ----, ----, 2016 WL 3002376, at *13-14 (E.D. Va. 2016). *Contra Levin*, --- F. Supp. 3d at ----, 2016 WL 2596010, at *10-12.

18

[*see* R. 24 at 14], the FBI agents acted with a good-faith, objectively-reasonable belief as to the validity of the NIT warrant. In this investigation, the agents diligently gathered evidence over a span of months before filing a detailed affidavit before a federal magistrate judge. [*See* R. 24-2 at 5-37.] An experienced and neutral magistrate judge then reviewed "the warrant application and concluded that there existed probable cause" to issue the NIT warrant. *Matish*, --- F. Supp. 3d at ----, 2016 WL 3545776, at *25.

True enough, Magistrate Judge Buchanan misapprehended the limits on her jurisdiction. The exclusionary rule, however, is designed "to curb police rather than judicial misconduct." *Master, 614 F.3d at 242* (quoting *Herring, 555 U.S. at 142* **[*23]**). Had the FBI agents deliberately or recklessly invited Magistrate Judge Buchanan to make that error, then suppression might be appropriate. *See Leon, 468 U.S. at 923* (finding good-faith exception inapplicable if law-enforcement officers knowingly or recklessly mislead judge to obtain a warrant). In this case, though, the FBI agents "provided the magistrate with all the information she needed to 'satisfy [herself] of [her] jurisdiction before proceeding.'" *Werdene*, --- F. Supp. 3d at ----, 2016 WL 3002376, at *16 (alterations in original) (quoting *Packard v. Provident Nat'l Bank, 994 F.2d 1039, 1049 (3d Cir. 1993)*).

The FBI agents can hardly be faulted for failing "to understand the intricacies of the jurisdiction of federal magistrates." *Darby*, --- F. Supp. 3d at ----, 2016 WL 3189703, at *14; *cf. Leon, 468 U.S. at 921* ("In the ordinary case, an officer cannot be expected to question the magistrate's . . . judgment that the form of the warrant is technically sufficient."). After all, there is disagreement among reasonable jurists on that very question. *Compare Henderson*, 2016 WL 4549108, at *3-4 (holding magistrate

19

judge lacked authority to issue NIT warrant under *Rule 41(b)(4)*), *and Adams*, 2016 WL 4212079, at *6 (same), *and Werdene*, --- F. Supp. 3d at ----, 2016 WL 3002376, at *7 (same), *and Levin*, --- F.

Supp. 3d at ----, 2016 WL 2596010, at *6 (same), *and* Arterbury, 2016 U.S. Dist. LEXIS 67091, at *21-22 (same), *and Michaud*, 2016 WL337263, at *6, *with Laurita*, 2016 WL 4179365, at *6-7 (holding magistrate judge had authority to issue NIT warrant under *Rule 41(b)(4)*), *and Matish*, --- F. Supp. 3d at ----

, 2016 WL 3545776, at *17-18 (same), *and Darby*, --- F. Supp. 3d at ----, 2016 WL 3189703, at *11-12 (same). "The fact that courts are presently divided over" whether the NIT warrant "even violated *Rule 41* is compelling evidence that the FBI did not . . .

deliberately violate the Rule by seeking the warrant in the first instance." *Acevedo-Lemus*, 2016 WL 4208436, at *7.

Exclusion "cannot 'pay its way'" under these circumstances. *Davis, 564 U.S. at 238* (quoting *Leon, 468 U.S. at 907 n.6*). The agents' conduct, if blameworthy at all, involved "only simple, 'isolated' negligence," while the costs of exclusion are **[*24]** substantial. *Id.* (quoting *Herring, 555 U.S. at 137*). Suppression would exclude "reliable, trustworthy evidence bearing on [Ammons'] guilt or innocence," *id. at 237* (citing *Stone v. Powell*, 428 U.S. 465, 490-91 (1976)), of a crime society has a significant "interest indeterring," *United States v. Bradley, 488 F. App'x 99, 104 (6th Cir. 2012)* (citing *United States v. Moore, 916 F.2d 1131, 1139 (6th Cir. 1990)*). Accordingly, the Court has notrouble concluding that suppression is unwarranted.

20

IV.

IT IS HEREBY ORDERED that Dennis Ammons' Motion to Suppress, [R. 24],

is **DENIED**.

IT IS SO ORDERED.

Date: September 14, 2016

cc: Counsel of Record

21

End of Document