IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

UNITED STATES OF AMERICA,

Plaintiff,

v. Case No. 17-10087-1-JTM

DANIEL EUGENE COOKSON,

Defendant.

MEMORANDUM AND ORDER

The instant prosecution is the result of an FBI investigation into Playpen, a website that facilitated the distribution of child pornography. Through a series of events, the FBI learned that defendant accessed Playpen from his home, and the government charged defendant with two counts of possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). Presently before the court is defendant's motion to dismiss (Dkt. 14) alleging that the government committed outrageous conduct. Defendant also moves to suppress all evidence derived from the search of his home computer, subsequent search of his residence, and statements made to the FBI (Dkt. 13). Defendant further moves for discovery (Dkt. 15). For the reasons stated below, defendant's motions to dismiss and suppress evidence are denied. Defendant's motion for discovery is denied without prejudice.

I. Background[1]

Playpen operated on the "The Onion Router" or "Tor" network, which provides more anonymity to its users than the regular Internet. The Tor was developed by the U.S. Naval Research Laboratory and is now accessible to the general public. Tor users must download special software that lets them access the network. When a user accesses the Tor, communications from that user are routed through a system of network computers that are run by volunteers around the world. When a user connects to a website, the only Internet Protocol ("IP") address that the website "sees" is the IP address of the last computer through which the user's communications were routed. This final relay is called an exit node. Because there is no practical way to trace a user's communications from the exit node back to the user's computer, Tor users are effectively anonymous to the websites they visit.

The Tor also provides anonymity to the individuals who run websites or forums on it. Websites may be set up on the Tor as "hidden services" that are only accessed through the Tor. The IP address is replaced with a Tor-based address, which consists of a series of alphanumeric characters followed by ".onion." There is no way to look up the IP address of the computer hosting a hidden service.

Tor users cannot simply perform a search to find a hidden service that may interest the user. Instead, a user must know the Tor-based address of the hidden service. As a result, a user cannot simply stumble onto a hidden service. The user may

[1] The majority of this background information is taken from the warrant application and supporting affidavit attached to defendant's motion to suppress (Dkt. 13-1).

obtain the address from postings on the Internet or by communications with other Tor users. One hidden service may also link to another.

Playpen was a hidden service contained on the Tor, and it had been linked to by another hidden service that was dedicated to child pornography. In December 2014, a foreign law enforcement agency informed the FBI that it suspected a United States-based IP address belonged to Playpen. In January 2015, after obtaining a search warrant, the FBI seized the IP address and copied the contents of the website. On February 19, 2015, the FBI arrested the individual suspected of administering Playpen.

The FBI seized control of Playpen, however, it could not easily identify Playpen users. Thus, the FBI obtained a warrant from an E.D. Va. magistrate judge allowing them to use a network investigative technique ("NIT") to locate the administrators and users of Playpen—including installing software onto the FBI's Playpen server in Virginia. The NIT installed itself as soon as a user logged into Playpen and reached the landing page; installation did not require any confirmed downloads of child pornography. Once installed, the NIT would search the user's computer for identifying information, such as the IP address, and transmit this information back to the FBI via the Playpen server located in the E.D. Va.

The FBI operated Playpen with the NIT from approximately February 20, 2015, to March 4, 2015. On February 22, 2015, a visitor named "shishkabobs" logged into Playpen, and the NIT was installed on shishkabobs's computer.

On March 26, 2015, the FBI used some of the data it had collected from shishkabobs's computer to obtain an administrative subpoena for Southern Kansas

Telephone Company, Inc. to identify the address. The telephone company provided the FBI with defendant's address in Howard, Kansas. Defendant's brother was the subscriber name on the internet account.[2]

On June 17, 2015, Judge Gale authorized a warrant for the FBI to search defendant's residence. Two days later, the FBI executed the search warrant and interviewed defendant at the county jail. Defendant provided a *Mirandized* confession regarding his use of Playpen and child pornography found on his devices. Approximately two years later, defendant was indicted on two counts of possession of child pornography.

II. Outrageous Conduct

Defendant asserts that the government acted outrageously when it operated Playpen without filters or limitations, thereby aiding and abetting at least 100,000 users in posting, viewing, and sharing illegal pictures and videos. Defendant is not arguing entrapment, but that the government's conduct was so inexcusable that it can only be described as outrageous.

A defendant may challenge the government's conduct during an investigation when it is sufficiently outrageous. The outrageous conduct defense is predicated on the Due Process Clause of the Fifth Amendment to the United States Constitution. If the government's conduct is deemed "outrageous," then it is not allowed to prosecute offenses developed through that conduct. The defense of outrageous conduct is distinct from the defense of entrapment, which looks at the defendant's state of mind to

[2] At the relevant time, both defendant and his brother resided with their parents in Howard, Kansas.

determine whether he was predisposed to commit the crime for which he is prosecuted. *United States v. Mosley*, 965 F.2d 906, 909 (10th Cir. 1992). In contrast, the outrageous conduct defense looks at the government's behavior. *Id.*

Other district courts have considered this claim and found that although the government's investigation and operation of Playpen had disturbing consequences, the government's conduct was not so outrageous as to warrant dismissal. *See, e.g.*, *United States v. Pawlak*, 237 F. Supp. 3d 460, 471 (N.D. Tex. 2017) (holding that the government did not violate the defendant's due process rights); *United States v. Hammond*, No. 16-CR-00102-JD-1, 2016 WL 7157762, at *6 (N.D. Cal. Dec. 8, 2016) ("While unsavory, the government's conduct did not rise to the level of outrageousness needed to support the dismissal of defendant's indictment."); *United States v. Owens*, No. 16-CR-38-JPS, 2016 WL 7079617, at *5 (E.D. Wis. Dec. 5, 2016) ("The Court is confident, however, that the government's actions in this matter were not so outrageous as to justify the dismissal of the indictment against Mr. Owens."); *United States v. Allain*, 213 F. Supp. 3d 236, 253 (D. Mass. 2016) ("Reasonable minds will no doubt differ on whether the government made the right choice here, but it is not the rare case in which any misconduct on the part of the government was sufficiently blatant, outrageous, or egregious to warrant the dismissal of the indictment.").

The court agrees with these decisions and finds that the government's conduct was not so outrageous as to support dismissing defendant's charges.

III. Motion to Suppress

Defendant challenges the initial warrant issued by the E.D. Va. magistrate,[3] and claims it was invalid under Federal Rule of Criminal Procedure 41 because it exceeded the magistrate's jurisdiction.[4]

The NIT warrant has already been subject to significant judicial scrutiny across the country. A majority of courts have found that the magistrate judge who issued the NIT warrant lacked authority to do so, yet declined to suppress the resultant evidence. *See, e.g.*, *United States v. Ammons*, No. 3:16–CR–00011–TBR–DW, 207 F. Supp. 3d 732, 2016 WL 4926438 (W.D. Ky. Sept. 14, 2016); *United States v. Henderson*, No. 15–CR–00565–WHO–1, 2016 WL 4549108 (N.D. Cal. Sept. 1, 2016); *United States v. Michaud*, No. 3:15–CR–05351–RJB, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016). A minority of district courts have suppressed evidence based on a finding that the warrant was void and the good-faith exception to the exclusionary rule did not apply. *See, e.g.*, *United States v. Levin*, No. CR 15–10271–WGY, 186 F. Supp. 3d 26, 2016 WL 2596010 (D. Mass. May 5, 2016); *United States v. Croghan*, No. 1:15–CR–48, 209 F. Supp. 3d 1080, 2016 WL 4992105

---

[3] Defendant argues that evidence from the subsequent search of his residence and his statements should be suppressed because they derived from the illegal installation of the NIT malware on his computer pursuant to *Wong Sun v. United States*, 371 U.S. 471 (1963). However, he is not directly challenging the validity of the residential warrant and interrogation.

[4] Fed. R. Crim. P. 41 has been amended and now permits magistrate judges to issue warrants such as the NIT warrant. It now reads:

> [A] magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if: (A) the district where the media or information is located has been concealed through technological means . . . .

Fed. R. Crim. P. 41(b)(6).

Because this amendment became effective on December 1, 2016, however, it does not apply to defendant's case. *United States v. Walker-Couvertier*, 860 F.3d 1, 9 (1st Cir. 2017).

(S.D. Iowa Sept. 19, 2016). But these district courts were reversed by their respective circuits, which held that the good-faith exception applied. *See, e.g.*, *United States v. Levin*, ---F.3d---, 2017 WL 4855774, at *1 (1st Cir. Oct. 27, 2017); *United States v. Horton*, 863 F.3d 1041, 1052 (8th Cir. 2017).

Recently, the Tenth Circuit bypassed directly deciding whether the E.D. Va. magistrate judge lacked authority to issue the warrant and held that even if the warrant should not have been issued, the good-faith exception to the exclusionary rule applied. *United States v. Workman*, 863 F.3d 1313, 1317, 1320–21 (10th Cir. 2017) ("[I]n our view, the executing agents acted in an objectively reasonable manner."). "Under the *Leon* exception, improperly obtained evidence remains admissible when the executing agents 'act with an objectively 'reasonable good-faith belief' that their conduct is lawful or when their conduct involves only simple, 'isolated' negligence. . . .'" *Workman*, 863 F.3d at 1317 (quoting *United States v. Leon,* 468 U.S. 897, 909 (1984) and *Davis v. United States*, 564 U.S. 229, 238 (2011)).

Defendant argues that the FBI was aware of the fact that Playpen had members throughout the world. Therefore, the executing officers knew the warrant would be invalid under the jurisdictional limitations of Rule 41 and/or the Federal Magistrates Act. Defendant contends that because "this warrant was approved at the highest levels of the FBI and the Department of Justice" the government cannot show they had a good-faith belief that the warrant was valid. (Dkt. 29, at 3).

The court finds that the E.D. Va magistrate exceeded her authority in issuing the warrant for the NIT. The court recognizes that the FBI's knowledge regarding the

validity of the warrant might cut against the government's position that the agents believed the warrant was proper. Nevertheless, the court is required to follow Tenth Circuit precedent and determines that *Workman* governs the outcome of defendant's motion. The underlying facts surrounding the E.D. Va. magistrate's authorization of the warrant and the FBI's conduct have not changed. Therefore, in accordance with *Workman*, the court finds that the good-faith exception to the exclusionary rule applies to the NIT search of defendant's computer and subsequent search of his residence.

IV. Motion for Discovery

Defendant moves for the court to order the government to provide him with a copy of the programming code for the NIT that was deployed on defendant's computer. Defendant also requests records relating to the government's review and approval of Operation Pacifier. Defendant argues that the NIT software can cause alterations in a computer's security settings permitting the computer to be exposed not only to the NIT, but to other malware or viruses that could explain why some or all of the alleged illegal materials were present on that computer. Because of this possibility, defendant requests a complete copy of NIT source code and all NIT components—including the exploit, payload server, and identifier components—used to identify Mr. Cookson's computer and any supporting documentation that could aid in understanding how the code works.

The government responds that it does not plan on using the NIT source code in its case-in-chief and further that it was not obtained from nor belonged to defendant. The government states that the NIT source code is subject to law enforcement privilege.

It also notes that the information collected by the NIT from defendant and his devices are available for defense counsel's review.

Defendant's discovery requests are denied without prejudice. All information and devices obtained from and belonging to defendant are available for review. Defendant's counsel and expert can review that information and determine whether there are materials that were not collected by and/or do not belong to defendant.

IT IS THEREFORE ORDERED this 22nd day of November, 2017, that defendant's motion to suppress (Dkt. 13) and motion to dismiss the indictment (Dkt. 14) are denied. Defendant's motion for discovery (Dkt. 15) is denied without prejudice.

s/ J. Thomas Marten
J. THOMAS MARTEN, JUDGE