United States v. Spicer

Decided Jan 31, 2018

Judge Susan J. Dlott

Order Denying Defendant's Motion for Disclosure of Discovery, Motion to Suppress Based on Unconstitutional Deployment of Government Sponsored Malware Dubbed the "Network Investigative Technique," and Second Motion to Suppress Evidence and Motion for *Franks* Hearing

This case stems from a highly-publicized FBI sting operation through which the FBI covertly deployed software called "Network Investigative Technique" or "NIT" onto computers that accessed a child pornography website called "PlayPen." Defendant Brandon Spicer was an individual who allegedly accessed the PlayPen website during this operation, which resulted in this prosecution at hand.

Three defense motions are pending before the Court: Motion for Disclosure of Discovery (Doc. 39), Motion to Suppress Based on Unconstitutional Deployment of Government Sponsored Malware Dubbed the "Network Investigative Technique" (Doc. 40), and Second Motion to Suppress Evidence and Motion for *Franks* Hearing (Doc. 64). For the reasons that follow, all three motions will be **DENIED.**

2 *2 ## I. Background

A. Facts

In 2014, FBI agents began investigating the PlayPen website suspected to harbor child pornography.[1] (Macfarlane Aff., Doc. 40-1 at PageID 187-90, ¶¶ 7-11.)[2] PlayPen operated on an anonymous network referred to as the "Tor" network. (*Id.* at PageID 187, ¶ 7.) Once logged in to the PlayPen website, a visitor could view the content of the site, which included discussion forums, a private messaging service, and images of child pornography. (Whalen Aff., Doc. 44-1 at PageID 381-86, ¶ 11-25.)

1 [3] The PlayPen website was initially referred to by law enforcement as "Website A" when maintaining the site's confidentiality was an issue. As confidentiality is no longer a concern, the Court will refer to the website by its actual name, PlayPen. (*See, e.g.*, Doc. 40-1 at PageID 179, n.1.)

2 Special Agent Douglas Macfarlane swore to the facts contained in his Affidavit in Support of Application for Search Warrant ("Macfarlane Affidavit") submitted in support of the Search Warrant Application authorizing the NIT deployment (the "NIT Warrant") in the United States District Court for the Eastern District of Virginia. (Doc. 40-1.)

3 Special Agent James R. Whalen swore to the facts in the Affidavit in Support of Application for Search Warrant ("Whalen Affidavit"), which was submitted to Magistrate Judge Stephanie K. Bowman in support of the Application for a Search Warrant of Brandon Spicer's home. (Doc. 44-1.)

After uncovering the suspected IP address for the PlayPen website, the government seized the server that hosted the site and placed a copy of the server onto a government-controlled server in Virginia. (*Id.* at PageID 381-82, ¶ 11.) On February 20, 2015, prosecutors in the Eastern District of Virginia submitted an application and affidavit for a search warrant to United States

Magistrate Judge Theresa Carroll Buchanan in Alexandria, Virginia, which she signed.[4] (Doc. 40-1 at PageID 208.) This warrant - the "NIT Warrant" -is the source of much debate and litigation, as is the Affidavit that supports the NIT Warrant sworn to by Special Agent Macfarlane.

[4] Prosecutors also applied for an order under the Wiretap Act, 18 U.S.C. §§ 2510, *et seq.*, to authorize the interception of communications on PlayPen. (Doc. 40-2.) United States District Court Judge Anthony J. Trenga signed the wiretap order the same day. (*Id.* at PageID 267.)

Macfarlane's Affidavit explained that in order to identify users of PlayPen, the government would need to deploy a software called NIT. (*Id.* at PageID 200-204, ¶¶ 31-37.) The NIT software would be sent to a user's computer anytime a visitor to PlayPen entered a username and password to access the site, and, in turn, would collect information from the user's computer and transmit the information to the FBI. (*Id.*)

According to data obtained in the wake of the deployment of the NIT, on February 22, 2015 Spicer logged on and accessed content on the PlayPen website under the username "MAZTER." (Doc. 44-1 at PageID 388-90, ¶¶ 32-43.) He had registered an account on PlayPen the previous August 23, 2014, from which time until March 3, 2015, he spent a total of 126 active hours on the site. (*Id.* at PageID 388, ¶ 30.)

On July 8, 2015, Magistrate Judge Stephanie K. Bowman authorized a search warrant of Spicer's residence, which was executed the following day. (Doc. 44-1.) Spicer's laptop, cell phone, and other property were seized at this time, and, in connection with the search warrant being executed, he made inculpatory statements.

B. Procedural History

On July 15, 2015, Spicer was charged in a three-count Indictment for receipt of child pornography in violation of 18 U.S.C. §§ 2252(a)(2) and 2252(b)(1) (Count 1), possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(4) and 2252(b)(2) (Count 2), and access with intent to view child pornography in violation of 18 U.S.C. §§ 2252(a)(4) and 2252(b)(2) (Count 3). (Doc. 14.)

On June 13, 2016, Spicer filed a Motion for Disclosure of Discovery (Doc. 39) and a Motion to Suppress Based on Unconstitutional Deployment of Government Sponsored Malware Dubbed the "Network Investigative Technique" (Doc. 40). On December 29, 2017, he filed a [*4] Second Motion to Suppress Evidence and Motion for *Franks* [5] Hearing (Doc. 64). On January 23, 2018, the Court held a hearing on the pending motions.

[5] [6]*Franks v. Delaware*, 438 U.S. 154 (1978).

[6] At the hearing, counsel for the Defendant argued the two suppression motions and rested on the papers for the discovery motion. Defendant also argued his Motion for Bond Reconsideration (Doc. 69), which the Court orally granted at the hearing. (Jan. 23, 2018 Docket Entry.)

II. Defendant's Pending Motions

A. Other Similar Cases

Defendant's three motions raise complex legal issues, all of which have been thoughtfully considered by other Judges in our district and beyond. *See United States v. Schuster*, 1:16-cr-051 (Order, Mar. 28, 2017) (Black, J.) (denying defendant's motion to suppress); *United States v. Gaver*, 3:16-cr-088, 2017 WL 1134814 (Decision and Entry, Mar. 27, 2017) (Rice, J.) (denying defendant's motions to suppress, motion for discovery, and motion for *Franks* hearing); *United States v. Jones*, 3:16-cr-026 (Decision and Entry, August 28, 2017) (Rose, J.) (denying motion to compel NIT source code), (Decision and Entry, August 18, 2017) (denying motion for *Franks* hearing), (Entry and Order, Feb. 2, 2017) (denying in part motion to suppress and amended motion to suppress); and *United States v. Stamper*, 1:15-cr-109 (Opinion & Order, Feb. 19, 2016) (Barrett, J.) (denying defendant's motion

to dismiss or alternatively suppress evidence). In addition, a number of Circuit Courts have ruled on the suppression issue. *See United States v. Levin*, 874 F.3d 316 (1st Cir. 2017) (finding the good faith exception to the exclusionary rule applied to preclude suppression); *United States v. Horton*, 863 F.3d 1041 (8th Cir. 2017) (finding the magistrate judge lacked jurisdiction to issue the NIT warrant, but the good faith exception precluded suppression); and *United States v. Workman*, 863 F.3d 1313 *5 (10th Cir. 2017) (finding that even if the warrant was invalid, the good faith exception precluded suppression).

The Court will adopt the reasoning set forth in Judge Rice's opinion in *Gaver*, as it persuasively addresses not only the issue of suppression, but also the request for discovery of the NIT source code and a request for a *Franks* hearing. In addition, the facts underpinning Gaver's prosecution are very similar. Gaver was charged with numerous counts of possession of child pornography, knowingly accessing with intent to view child pornography, and knowing receipt of child pornography. *Id.* at *1. The government deployed NIT onto Gaver's computer after he logged onto the PlayPen website during the period in time when the government was operating the site from a server in Virginia for the purpose of its investigation. *Id.* After obtaining Gaver's IP address and uncovering Gaver's identity, a warrant was obtained to search his apartment in Dayton, Ohio, which uncovered computers and other items. *Id.* Like Spicer, Gaver filed a Motion to Suppress Evidence Based on Unconstitutional Deployment of Government-Sponsored Malware Dubbed the "Network Investigative Technique," a Motion for Disclosure of Discovery, and a Second Motion to Suppress Evidence and Motion for *Franks* Hearing. *Id.* All three motions were denied.

With this framework in mind, the Court will briefly consider Defendant's motions and apply *Gaver*'s analysis to each.

B. Motion for Disclosure of Discovery

Spicer moves the Court for an order compelling the government to disclose the components of the NIT source code, including the payload, exploit, identifier, and server *6 components.[7] In *Gaver*, when a virtually identical motion was filed, the Court found that the items requested were not material to Gaver's defense, and, regardless, they were subject to the law enforcement privilege. [8]*Id.* at *3. The Court concludes that the same reasoning applies here. Spicer has not demonstrated that the requested materials are material to his defense. Even he had, the law enforcement privilege applies, as disclosure of the exploit and server component would severely compromise future investigations and could allow others to develop counter-measures. *Id.* at *3-4. Defendant's Motion for Disclosure of Discovery (Doc. 39) is, therefore, **DENIED.**

[7] Spicer also seeks a copy of the PlayPen homepage as it appeared on February 20, 2015 when the government sought the NIT warrant, but it has since been provided (and was the impetus for Spicer's Second Motion to Suppress and Motion for *Franks* Hearing (Doc. 64)).

[8] Federal Rule of Criminal Procedure 16(a)(1)(E) requires the government to permit inspection of items within its control if: (1) the item is material to defense preparation; (2) the government intends to use it in its case-in-chief, or (3) the item was obtained from or belongs to the defendant. *Id.* at *3.

C. Motion to Suppress Based on Unconstitutional Deployment of Government Sponsored Malware Dubbed the "Network Investigative Technique"

Spicer moves the Court to suppress all evidence flowing from the Government's deployment of the NIT software on his computer, including the search of his home and statements obtained from him. Spicer argues that the deployment was an illegal search under the Fourth Amendment. He contends the Magistrate Judge

had no authority under the Federal Magistrates Act, 28 U.S.C. § 636, or Federal Rule of Criminal Procedure 41 to authorize a search outside the boundaries of the Eastern District of Virginia. Under Rule 41, a magistrate judge is authorized to authorize a search in limited circumstances,[9] none of which apply, rendering the *7 NIT Warrant *void ab initio*. Suppression, Spicer argues, is the appropriate remedy. Even if the Court were to find that the NIT Warrant was issued without judicial authority and was a technical violation of Rule 41, as opposed to a violation of his Fourth Amendment rights, the evidence should still be suppressed, because he was prejudiced.

7

[9] Federal Rule of Criminal Procedure 41(b) reads as follows: (**b**) **Venue for a Warrant Application.** At the request of a federal law enforcement officer or an attorney for the government: (**1**) a magistrate judge with authority in the district -- or if none is reasonably available, a judge of a state court of record in the district -- has authority to issue a warrant to search for and seize a person or property located within the district; (**2**) a magistrate judge with authority in the district 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 but might move or be moved outside the district before the warrant is executed; (**3**) a magistrate judge--in an investigation of domestic terrorism or international terrorism--with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district; (**4**) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and (**5**) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:

> (**A**) a United States territory, possession, or commonwealth;
>
> (**B**) the premises--no matter who owns them--of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or
>
> (**C**) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

Subdivision (b)(6), repeated below, was added pursuant to a 2016 amendment: (**6**) 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; or
>
> (**B**) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

In opposition, the government argues that (1) Spicer did not have a reasonable expectation of privacy in his IP address and therefore no search occurred; (2) even if a search did occur, the Magistrate Judge had authority under Rule 41(b)(4) to issue the NIT Warrant; (3) even if there was a Rule 41 violation, suppression is not the appropriate remedy; and (4) regardless, the evidence should not be suppressed under the good-faith exception of *United States v. Leon*, 468 U.S. 897 (1984).

8 *8 For the reasoning set forth more fully in *Gaver*, the Court concludes that the Magistrate Judge lacked authority under Rule 41(b) to issue the NIT Warrant, but determines that suppression is not an appropriate remedy for the violation. Rather, the *Leon* good-faith exception applies to save the NIT Warrant. *Id.* at *11-12. Defendant's Motion to Suppress Based on Unconstitutional Deployment of Government Sponsored Malware Dubbed the "Network Investigative Technique" (Doc. 40), accordingly, is **DENIED.**

D. Second Motion to Suppress Evidence and Motion for *Franks* Hearing

Spicer's Motion filed on December 29, 2017 asserts three additional grounds for suppression. First, Spicer argues that the Government intentionally or recklessly made false and misleading statements and omitted material facts in Macfarlane's Affidavit in support of the NIT Warrant, requiring suppression and a *Franks* hearing. Macfarlane averred that upon arrival at the PlayPen website, a user would see "images of prepubescent females partially clothed and whose legs are spread with instructions for joining the site before one can enter." (Doc. 40-1 at PageID 190, ¶ 10.) A later reference in his Affidavit likewise mentions "two images depicting partially clothed prepubescent females with their legs spread apart." (*Id.* at ¶ 12.) Discovery has revealed, however, that at the time he signed his Affidavit on February 20, 2015, the homepage instead included an image of a clothed female, with her legs crossed, who Defendant argues is not clearly "prepubescent." (*Compare* Doc. 68-2 *with* 68-3.) It is undisputed that the PlayPen homepage changed between February 18, 2015 and February 20, 2015. At oral argument, defense counsel referred to Macfarlane's testimony about his Affidavit in other cases and the fact that he failed to access the PlayPen website one last time prior to submitting his Affidavit. *See Gaver*, 2017 WL 1134814, at *5 (summarizing 9 Macfarlane's testimony about his Affidavit.) *9 Although other agents may have signed on to the PlayPen webpage on February 19, 2015 and observed the change, no one told Macfarlane about it. *Id.*

Second, Defendant argues that Macfarlane made false and misleading statements about the location of the NIT searches, as the NIT Warrant is limited to a location in the Eastern District of Virginia, and Spicer's computer was in Ohio at the time the NIT software was deployed. For these reasons, Spicer argues he is entitled to a *Franks* hearing.[10] Lastly, Spicer argues the NIT Warrant is an unconstitutional "general" warrant.

[10] In *Franks*, the Supreme Court held as follows:

> where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request. In the event that at that hearing the allegation of perjury or reckless disregard is established by the defendant by a preponderance of the evidence, and, with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit.

As to the change in the PlayPen website homepage, the Court has reviewed the differences between the two PlayPen homepages and agrees with Judge Rice that they are not materially different. Both include images that "are highly suggestive of the website's illegal contents, particularly when paired with the website's name, and the fact that it was accessible only through the Tor network." *Gaver*, 2017 WL 1134814 at *6. "In short, even with an accurate description of the website's logo[/images], probable cause would have existed for the issuance of the warrant." *Id.* The Court is not satisfied that the Defendant has shown the false statement was made knowingly and intentionally or with reckless disregard for the truth to warrant a *Franks* hearing. *Id.* at *5.

10 *10 The Court also disagrees with Spicer that Macfarlane's Affidavit contained false and misleading statements about the location of the NIT searches for the reasons set forth by the Court in *Gaver*. Thus, Spicer is not entitled to a *Franks* hearing on this ground, either. *Id.* at *7. Finally, as in *Gaver*, the Court rejects the argument that the NIT Warrant is an unconstitutional "general" warrant. *Id.* at *13. For these reasons, Defendant's Second Motion to Suppress and Motion for Franks Hearing (Doc. 64) also is **DENIED.**

III. CONCLUSION

This Court adopts the ruling of Judge Rice in *United States v. Gaver*, 3:16-cr-088, 2017 WL 1134814 (Decision and Entry, Mar. 27, 2017), and, in so doing, **DENIES** all three of Defendant's pending motions: Motion for Disclosure of Discovery (Doc. 39), Motion to Suppress Based on Unconstitutional Deployment of Government Sponsored Malware Dubbed the "Network Investigative Technique" (Doc. 40), and Second Motion to Suppress Evidence and Motion for *Franks* Hearing (Doc. 64).

IT IS SO ORDERED.

s/Susan J. Dlott

Judge Susan J. Dlott

United States District Court

Id. at 155-56. To warrant a hearing, a defendant must accompany his or her allegations with an offer of proof, affidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained. Id. at 171. A statement is made "with reckless disregard for the truth" when viewing all the evidence, "the affiant in fact entertained serious doubts as to the truth of the affidavits or had obvious reasons to doubt the accuracy of the information contained therein." United States v.

Cican, 63 F. App'x 832, 835-36 (6th Cir. 2003) (citing United States v. Johnson, 78 F.3d 1258, 1262 (8th Cir. 1996)).