No. 17-30117

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

DAVID TIPPENS,

Defendant-Appellant.

On Appeal from United States District Court
Western District of Washington at Tacoma
District Court Case No. 3:16-cr-05110-RJB-1

The Honorable Robert J. Bryan
United States District Judge

# DEFENDANT-APPELLANT'S OPENING BRIEF

COLIN FIEMAN
*Assistant Federal Public Defender*

ALAN ZARKY
*Research & Writing Attorney*

Federal Public Defender Office
1331 Broadway, Suite 400
Tacoma, Washington 98402
(253) 593-6710

# TABLE OF CONTENTS

# TABLE OF AUTHORITIES

## Federal Cases

**Federal Statutes**



**Other**

## I. STATEMENT OF JURISDICTION

A. The District Court for the Western District of Washington had subject matter jurisdiction in this matter pursuant to 18 U.S.C. § 3231.

B. This Court has jurisdiction to hear this appeal pursuant to 28 U.S.C. § 1291.

C. The District Court's Judgment of Conviction was filed on June 13, 2017. ER.I 3. Appellant David Tippens filed a notice of appeal on June 14. ER.I 1. This appeal is timely because the notice of appeal was filed within ten days of the date on which the order was entered. Fed. R. App. P. 4(b)(1)(A)(I).

## II. BAIL STATUS

The District Court released Mr. Tippens pending appeal.

## III. ISSUES PRESENTED

A. Where the court below found that the Government committed outrageous and illegal misconduct by operating a massive child pornography website and needlessly re-victimizing hundreds of children, did the court err by not dismissing the indictment in this case as either a due process violation or under the court's supervisory powers?

B. When a Virginia magistrate judge authorized a search warrant for "Property located in the Eastern District of Virginia" and the Government instead

searched Mr. Tippens's computer in Hawaii, did that search exceed the scope of the warrant and require suppression?

C. When the trial court found that the Hawaii search also violated the then-existing version of Fed. R. Crim. P. 41(b) and the facts establish that the search was prejudicial, deliberate or of constitutional magnitude (and in fact all three), did the court err by not suppressing all fruits of that search?

D. When the Virginia warrant authorized the Government to search the computers of anyone who accessed the homepage of a website and the agents who prepared the warrant alleged in the supporting affidavit that the homepage displayed graphic images of minors when they knew that it did not, and the website did not otherwise advertise its nefarious purpose, did the trial court err in finding the falsehoods immaterial?

E. When a second warrant authorized the Government to search Appellant's computer a year after he visited the Government's website and after he had moved to another state, and the supporting application falsely alleged that illegal pictures and evidentiary data were stored on his computer, and then coupled those falsehoods with a boilerplate and misleading "collector profile," did the court below err in finding the falsehoods immaterial and not made intentionally or recklessly?

F. Can the Government invoke the good faith exception to the exclusionary rule to avoid suppression when it searched an unauthorized location, violated Rule 41 and made false statements and material omissions in its warrant applications and when the good faith exception does not apply to any of the Government's unlawful and unconstitutional actions?

## IV. STANDARD OF REVIEW

This Court reviews a due process claim of outrageous Government misconduct *de novo*; it reviews a claim under a court's supervisory powers for an abuse of discretion. *United States v. Fernandez*, 388 F.3d 1199, 1238 (9th Cir. 2004), *opinion modified*, 425 F.3d 1248 (9th Cir. 2005).

The Court reviews *de novo* the question of whether a violation of Rule 41(d) requires suppression. *United States v. Johns*, 948 F.2d 599, 603 (9th Cir. 1991).

Whether a search violates the Fourth Amendment is an issue of law and also reviewed *de novo*. *United States v. Stafford*, 416 F.3d 1068, 1073 (9th Cir. 2005).

The Court also reviews *de novo* a district court's determination "'whether probable cause is lacking because of alleged misstatements or omissions in the supporting affidavit.'" *United States v. Perkins*, 850 F.3d 1109, 1115 (9th Cir. 2017) (citation omitted). This Court reviews a finding that a search warrant "affidavit did not contain purposefully or recklessly false statements or omissions"

under the clearly erroneous standard. *Id.* at 1115. Findings of fact are reviewed for clear error. *United States v. Christie*, 825 F.3d 1048 (9th Cir. 2016).

## V. STATEMENT OF THE CASE

On March 10, 2016, Mr. Tippens was charged by Indictment with one count of receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2), and one count of possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4). Excerpts of Record Volume IV (ER.IV) 734. On August 22, 2016, he filed both a motion to dismiss the Indictment, based on outrageous Government conduct, ER.IV 717, and a motion to suppress evidence. ER.IV 679. The district court held a hearing on those two motions and another (which is not a subject of this appeal) beginning October 31, 2016, and denied the motions in a written order dated November 30, 2016. ER.I 36.

On January 18, 2017, the Government filed a Superseding Indictment, adding a charge of transportation of child pornography in violation of 18 U.S.C. § 2252(a)(1). ER.II 296. Mr. Tippens filed a second motion to suppress evidence on January 26, 2017. ER.II 269. The district court held a hearing on that motion on February 13, 2017, ER.II 109, then denied it in a written order dated February 16, 2017. ER.I 19.

A bench trial was held beginning March 13, 2017. On March 14, the court dismissed Counts 1 and 3 of the Superseding Indictment (the receipt and

transportation counts). ER.I 11, 18. The court convicted Mr. Tippens of Count 2 (possession) on March 15. On May 26, 2017, the court sentenced Mr. Tippens to six months custody and ten years supervised release. The court determined the conditions of supervised release on June 13, 2017, and issued its Judgment that day. ER.I 3. On June 14, 2017, Mr. Tippens filed a timely notice of appeal. ER.I 1. This appeal followed.[1]

## VI. SUMMARY OF THE ARGUMENTS

Mr. Tippens seeks dismissal of the indictment or reversal of his conviction because the Government committed outrageous misconduct during the undercover operation that led to two searches of Mr. Tippens's computer and the charges against him. In early 2015, the FBI operated a website called "Playpen" and became one of the world's largest distributors of child pornography. While operating the site, the FBI obtained a search warrant in Virginia and, despite the warrant's limited authorization, targeted thousands of computers around the world (including Mr. Tippens's) with a type of malware called a "network investigative technique" (NIT). The NIT was sent to anyone who visited Playpen and tried to

[1] This case was joined below with two related cases, *United States v. Lorente*, CR15-0274-MJP, and *United States v. Lesan*, CR15-0387RJB. These cases followed a fourth related case, *United States v. Michaud*, CR15-05351RJB. The Hon. Robert J. Bryan presided over all of these cases, and both the court and the parties incorporated some of the discovery, testimony, and pleadings from the *Michaud* case in Mr. Tippens's case below. Mr. Tippens's case is the only one before this Court.

access it. Meanwhile, the FBI distributed from its site one million or more images and videos of child abuse; needlessly upgraded the site and attracted 56,000 new users; facilitated the posting of thousands of images of child abuse; and, as the court below found, re-victimized hundreds of children. The trial court found "[i]t is easy to conclude that the Government acted outrageously here" and made multiple findings of misconduct, including violations of law. The Government's conduct was all the more egregious because it has previously been rebuked by a Court of Appeals for distributing pornography as part of a sting operation. *United States v. Sherman*, 268 F.3d 539 (7th Cir. 2001). The court below nevertheless declined to dismiss the indictment. This Court should reverse under its supervisory powers or as a matter of due process, both to sanction the Government's appalling actions and to deter similar future misconduct.

In addition, the Court should suppress all fruits of the NIT search of Mr. Tippens's computer because the Government obtained a single warrant in the Eastern District of Virginia and that warrant only authorized searches within the district. At the time of the NIT search in this case, Mr. Tippens was living in Hawaii. Where, as here, the Government searches a location not authorized by the warrant it is relying on, suppression is required. *See, e.g., United States v. Sedaghaty*, 728 F.3d 885, 915 (9th Cir 2013). Moreover, the good faith exception

does not apply when officers search an unauthorized location. *United States v. Gantt*, 194 F.3d 987 (9th Cir.1999).

The Government also violated Fed. R. Crim. P. 41, which has the force of law, when it searched Mr. Tippens's Hawaii computer. The version of Rule 41 in effect at the time of the NIT searches did not allow magistrate judges to issue warrants for locations outside a judge's district, except in terrorism cases. Although the Government was fully aware of these jurisdictional restrictions (and, consistent with them, the judge limited her authorization to Eastern Virginia), the FBI hacked into computers not only in Hawaii but in 120 other countries as well.

This Court has held that suppression is required whenever a violation of Rule 41 is prejudicial, deliberate or of constitutional magnitude. *United States v. Weiland*, 420 F.3d 1062 (9th Cir. 2005). In this case, the search was all three, yet the court below did not follow *Weiland*, found the violation merely "technical," and declined to order suppression. This Court should reverse because that decision was manifestly wrong both as a matter of fact and law. In addition, the good faith exception does not apply to the rule violation, particularly because the violation was deliberate.

The Government also made false statements in the Virginia warrant application that were central to the magistrate judge's finding of probable cause and it knew the statements were false before submitting the application.

Specifically, probable cause to search the computers of Playpen visitors, including people who had never visited the site before, depended on the appearance of the site's homepage. Unless the homepage advertised its nefarious purpose clearly enough that any visitor would recognize that purpose, there was no basis to conclude that 100,000 or more Playpen visitors were likely committing a crime. Accordingly, the Government alleged in its application that Playpen advertised itself as a child pornography site and displayed explicit pictures of prepubescent girls on its homepage.

In fact, Playpen did not advertise or preview its contents, there were no pictures of "prepubescent girls" or other explicit images on its homepage, and the homepage was unremarkable. Moreover, the lead FBI agent and administrator of Playpen, who also helped prepare the Virginia warrant application, admitted he knew the site description was false before the application was submitted. Nevertheless, the court below relied on the false description to find probable cause, and then concluded that the falsehoods were "immaterial." This Court should reject those erroneous conclusions, excise the false statements, find there was no probable cause without them, and order suppression. *Franks v. Delaware*, 438 U.S. 154 (1978).

The Government also made material false statements in connection with a second warrant to search Mr. Tippens's home in Washington, where he was

transferred by the Army several months after the Hawaii NIT search. In its warrant application, a year after the NIT search, the Government alleged that Mr. Tippens's computer had automatically stored Playpen pictures and related data while either Mr. Tippens or another resident of his house was visiting the site. In fact, Playpen operated on the "Tor" network, and Tor has automatic security features that prevent storage of images and related data on users' computers while visiting websites. The affiant admitted during cross-examination below that he knew of these security features before he applied for the Washington warrant but omitted all the relevant technical facts from his affidavit.

Because the Government waited a year to search Mr. Tippens's home, after he had moved to a new state, the application's false data storage claims were material. Without them there is no nexus between the alleged criminal activity and the search location. This is particularly true because the only other part of the application that purportedly established a nexus was a "collector profile," but that profile was both foundationless and misleading. The affiant admitted below the profile was "boilerplate." It also contained no facts showing Mr. Tippens fit the profile, and it was affirmatively misleading because it omitted inconsistent information about the habits of Tor users that the Government had alleged elsewhere. Nevertheless, the court below credited the profile and found it bolstered the affiant's misstatements and omissions about Tor and long term data storage.

This Court should conclude, however, that the profile was foundationless and affirmatively misleading; excise it from the Washington application; and find that the remaining facts in the application are stale and attenuated, thereby requiring suppression. *Franks*, *supra*.

## VII. STATEMENT OF FACTS

### A. THE TOR NETWORK AND OPERATION PACIFIER

This case arises from an FBI investigation called "Operation Pacifier." The investigation began in December, 2014, when the FBI obtained an internet protocol (IP) address associated with a website called Playpen.[2] ER-S (Sealed Excerpts of Record) volume V 943-44. Playpen operated on the Tor network (an acronym for "the onion router"), which is designed to route online communications through multiple computers (or "nodes") to anonymize IP addresses and other identifying information. ER-S.V 932-34; *see also* ER-S.VI 1049-82 (Testimony of Dr. Chris Soghoian explaining how Tor functions).[3]

---

[2] An IP address "refers to a unique number used by a computer to access the Internet" and is "also used by computer servers, including web servers, to communicate with other computers." ER-S.V 930-31. The address is assigned by an Internet Service Provider (ISP). *Id.*

[3] *See also* https://www.torproject.org ("Tor is free software and an open network that helps you defend against traffic analysis, [which is] a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.").

Tor was originally designed by the U.S. Naval Research Laboratory and is largely funded by the U.S. government. *See* Alex Hern, U.S. Government Increases Funding for Tor, The Guardian, July 29, 2014.[4] It is readily accessible with free software. ER-S.V 932-33. Tor is used by millions of people and, like the Internet in general, Tor can be used for both legitimate and illicit purposes. *See* ER.II 210 (referencing the Tor project's estimate of 40,000,000 users); Virginia Heffernan, Granting Anonymity, N.Y. Times, December 17, 2010 ("Peaceniks and human rights groups use Tor, as do journalists, private citizens and the military, and the heterogeneity and farflungness of its users — together with its elegant source code — keep it unbreachable.").[5] The Department of Justice (DOJ) has recommended that federal judges use Tor to protect their online communications. Joseph Cox, Department of Justice Official Tells Hundred Federal Judges to Use Tor, Motherboard.com, August 6, 2016.[6]

Playpen's IP address was revealed when there was a "misconfiguration" that allowed investigators to collect address information not normally accessible.

---

[4] Available at: https://www.theguardian.com/technology/2014/jul/29/us-government-funding-tor-18m-onion-router

[5] Available at: http://www.nytimes.com/2010/12/19/magazine/19FOB-Medium-t.html?_r=0

[6] Available at: https://motherboard.vice.com/en_us/article/xyg45n/department-of-justice-official-tells-hundred-federal-judges-to-use-tor

ER- S.V 1029 at n. 4. Following up on this information, the FBI identified and arrested the original administrator of the site in Florida on February 19, 2015. ER- S.V 944-45. FBI agents, including lead Operation Pacifier Case Agent Daniel Alfin, searched the administrator's home and seized a computer displaying the Playpen site. ER-S.V 861; ER-S.VI 1099-1103. The FBI then took control of the site, moved it to a government server in Virginia, and applied for a search warrant the next day to search visitors' computers and seize identifying information from them. ER-S.V 944-45.

### B. THE FBI'S ADMINISTRATION OF PLAYPEN

From February 19, 2015, until March 5, 2015, the FBI operated Playpen as an undercover website. *See, e.g.*, ER-S.V 861, 1035 at ¶ 27. During this time, the FBI was one of the world's largest distributors of child pornography on the Internet, ultimately acquiring 214,898 Playpen "members" and approximately 100,000 active visitors while the site was under government control. ER-S.V 935 at ¶ 11, 1030 at ¶ 15. The FBI boosted membership in its site by more than 56,000 in just 15 days, an increase that was likely due to FBI improvements to Playpen's speed, accessibility, and the "file hosting" features that enabled users to post, download and redistribute images. *Id,* ER.I 43 (misconduct finding (3)); ER.III 527-28; ER.IV 656-678. Undercover agents, including Agent Alfin, posted announcements about some of these improvements on Playpen and elicited user

comments about how much better the site was operating. ER.IV 656-678; ER-S.V 861-62, 871-93.

While operating Playpen, the FBI maintained at least 67,000 pictures, videos and links on it, with no restraints on users' ability to copy and redistribute that content or post new images. ER-S.V 914-15. The FBI also enabled the uploading of 44 new series of child abuse pictures, containing images that had not previously circulated on the Internet. ER.I 40-41.

The Government had no protocols or guidelines for its handling or containment of child pornography on Playpen and did not track the distribution of the site's content. ER.III 527-30. However, a conservative estimate (based on the volume of that content and the number of visitor log-ins) is that the FBI distributed at least 1,000,000 pictures and videos, and likely far more. ER.IV 719-20; ER-S.V 915. The Government did not dispute this estimate below.

### C. THE VIRGINIA "NIT" SEARCH WARRANT

#### 1. The scope of the Virginia warrant

The day after seizing Playpen, the FBI obtained a warrant from a magistrate judge in the Eastern District of Virginia to search and seize "property located in the Eastern District of Virginia." ER-S.V 954. The warrant authorized the FBI to send a "network investigative technique" (NIT) from the Playpen server to target

computers and seize data about "any user or administrator who logs into [Playpen] by entering a username and password." ER-S.V 955.

NITs are a type of malware.[7] The warrant application described the NIT as "computer instructions" that would be unknowingly downloaded by the unidentified users while they accessed the site. ER-S.V 946 at ¶ 33. The "information to be seized" by the NIT from target computers included their IP addresses; their MAC addresses (unique identifiers that are stored on a computer, *see* ER-S.V 1026 at ¶ 7(q)); the computers' "usernames"; and other data. ER-S.V 946-48. The application explained that there was no way for the Government to obtain IP addresses from ISPs or other third parties. ER-S.V 933 at ¶ 8, 944 at ¶ 29.

Consistent with the warrant itself, the supporting application's cover sheet stated the FBI was seeking to search persons or property "located in the Eastern District of Virginia." ER-S.V 922. On page 29 of the application, however, the affiant stated that the NIT "may cause an activating computer - wherever located – to send to a computer controlled by or known to the government, network level

[7] Malware is short for "malicious software." It is "specifically designed to gain access or damage a computer without the knowledge of the owner. There are various types of malware including spyware, keyloggers, true viruses, worms, or any type of malicious code that infiltrates a computer." https://us.norton.com/internetsecurity-malware.html. *See also* ER-S.V 1060, 1068.

messages containing information that may assist in identifying the computer" and its location. ER-S.V 951 at ¶ 46(a).

The warrant itself did not incorporate the warrant application by reference, nor was the application physically attached to the warrant. *See* ER-S.V 954-56.

**2. The facts offered in support of the warrant**

The application described Playpen as a "message board website whose primary purpose is the advertisement and distribution of child pornography." ER- S.V 935 at ¶ 11. It also alleged that "upon arrival at the TARGET WEBSITE the user sees images of prepubescent females partially clothed and whose legs are spread along with instructions for joining the site before one can enter." ER-S.V 935 at ¶ 10; *see also* ER-S.V 935 at ¶ 12 (describing "two images depicting partially clothed prepubescent girls with their legs spread apart"). In fact, the homepage did not display pictures of "prepubescent girls" or any sexual images. ER-S.VI 1083 (the homepage). The site also did not advertise its contents. For example, the homepage contains no references to pornography or "Lolitas," or otherwise showed that it contained child pornography. *Id.* The name "Playpen" itself is associated with several mainstream "adult" sites, a knock-off of *Playboy* magazine, and strip clubs. ER.IV 706; ER-S.VI 1089-95.

The FBI knew before it submitted the warrant application that Playpen did not advertise its contents or display explicit images on its homepage. Lead Agent

Daniel Alfin had participated in the preceding raid of the original Playpen administrator's home in Florida and was an administrator of the site after it was moved to a government server. *See, e.g.*, ER-S.V 861, 871; ER-S.VI 1097-1111. During the Florida raid, Alfin examined the former administrator's computer and saw that the homepage displayed merely a single small picture of a young woman or older teenager, seated, clothed and unremarkable in appearance. ER-S.VI 1100-01.

Alfin also helped prepare the Virginia warrant application; it was submitted to the Virginia court the day after he and other agents took control of Playpen. ER.III 517; ER-S.VI 1102-03, 1109-10. The application notes it was reviewed by an Assistant United States Attorney before it was submitted. ER-S.V 946 (application cover sheet noting review by "AUSA Whitney Dougherty Russell"). In addition, the entirety of Operation Pacifier was approved and supervised by senior personnel at DOJ and the FBI. ER.III 515-17.

The application explained that many Tor sites "are not indexed like websites on the traditional Internet" and visitors had to know Playpen's address in order to visit it. ER-S.V 934 at ¶ 10. According to the affiant, this fact made it "extremely unlikely that any visitor could simply stumble upon [the site] without understanding its purpose and content." *Id.* In fact, there are a variety of search engines for Tor sites. *See, e.g.* Kristen Hubby, Here Are The 13 Best Deep Web

Search Engines, dailydot.co (Nov. 28, 2016).[8] Playpen visitors logged in by entering a username and password and the site advised them to avoid using personal information. ER-S.V 935-36 at ¶ 12. There was no membership fee; the site did not offer previews of its content; and visitors could make up a username and password on the spot to gain immediate access. *See* ER-S.V 937.

The application also described how visitors navigated the site once they gained access to it. After leaving the homepage, visitors were presented with a directory or index of topics, some with names like "general discussion" and "fiction," but most with such titles as "girls HC" and "preteen-boy." ER-S.V 936-38. The index page, like the homepage, did not display any pornography. Instead, visitors had to take the additional steps of selecting a folder and opening it to see what it contained, which in most cases was child pornography. *See id*.

After describing Playpen and the Tor network, the application sought authorization to search the computer of "any user who logs into the TARGET WEBSITE" and refers to them as "activating computers." ER-S.V 948 at ¶¶ 35-36. The application contained no individualized information about users and the warrant authorized the FBI to deploy the NIT against any and all visitors while they were in the process of logging into the site. ER-S.V 946 at ¶ 32; *see also* ER-S.VI at 1070-71.

[8] Available at: https://www.dailydot.com/layer8/best-deep-web-search-engines/

### 3. The NIT searches of Appellant's and thousands of other computers

The FBI searched Mr. Tippens's laptop with an NIT while it was located at his home in Hawaii. *See* ER-S.V 1035-37. Once the NIT infected his computer it did several things to locate and seize data. First, the NIT had an "exploit" component that took advantage of a vulnerability in Mozilla's popular Tor browser to penetrate the computer's operating system. The Government refused to disclose the NIT's source codes, so their exact capabilities and effects are unknown. However, the experts below agreed that "exploits" can alter or delete stored data in the process of gaining access to it. ER.III 436-41; ER-S.V 761-64: ER-S.VI 1112-45 (expert declarations explaining how NITs function); *see also* ER-S.V 906 (Congressional Research Service report on amendments to Rule 41 and risks associated with governmental use of malware and exploits). The available information about the NIT also indicates that "the Government exploited the very type of vulnerability that would allow third parties to obtain total control [of] an unsuspecting user's computer." ER.IV 541, 569 (Mozilla Motion to Intervene).

The NIT also had a "payload" component that searched a computer's files and operating system to locate the data that the Government sought. ER-S.VI 1112-14. Finally, the NIT overrode or bypassed the user's security settings and forced the computer to send seized data back to the FBI, where it was stored in the digital equivalent of an evidence room. ER-S.VI 1064-69, 1113-15.

The FBI ultimately seized 8,713 IP addresses and other identifying data from computers located throughout the United States and in 120 other countries, including Russia, Iran and China, as well as data from an entity the Government described as "a satellite provider." ER-S.V 863-64.

### D. THE WASHINGTON SEARCH WARRANT AND 2016 SEARCH OF MR. TIPPENS'S HOME

A year after the Government shut down Playpen, the FBI obtained a warrant in the Western District of Washington to search Mr. Tippens's home in University Place. ER-S.V 997-1008. The affidavit in support of the warrant alleged that a Playpen visitor with the user name "candygirl123" had been logged into Playpen for 26 hours over a three month period and during that time had viewed child pornography on two specific dates. ER-S.V 1035-36.

The first date was allegedly February 26, 2015, when the visitor "accessed" a post on the site that contained two explicit pictures of minors. The application stated that those pictures would have been "displayed on the user's computer screen upon accessing." ER-S.V 1036-37 at ¶ 33.

The second date was February 28, 2015, when "candygirl123" visited the site again and accessed a post which "contained an embedded image [that] is a compilation of 240 individual images" (or "thumbnails") that depict child pornography. ER-S.V 1037 at ¶ 34. According to the affidavit, a copy of the post was "displayed on the user's computer screen" while the user was viewing it. *Id*.

The affidavit further alleged that a second copy of the compilation was stored on the computer itself when the visitor clicked on it to view some of its contents, "which would have resulted in downloading *another copy* of the image *to the user's computer*." *Id*. (emphasis added). There is no allegation that the user intentionally copied or saved any Playpen pictures, or otherwise accessed or possessed child pornography. *See also* ER.II 216-18.

In fact, the affiant, Pierce County Sheriff's Dept. Det. Douglas Shook, knew that the pictures the visitor had viewed would not have been saved on the computer. In this regard, Shook admitted during the suppression hearing below that the Tor browser has a security feature known as "disc avoidance" that blocks the automatic storage of web content on a user's computer; he knew this before he submitted his affidavit; and he omitted the information from the affidavit. ER.II 168-177, 274-276; ER-S.V 761-764 (declaration of Prof. Matthew Miller explaining Tor's content blocking features).

Moreover, the Tor browser is designed to block the retention of data related to those images, such as website addresses. ER.II 170-71. While some "trace evidence" or "artifacts" (like a site address) may be retained by the computer, "trace" data is typically stored in short term "volatile" or "random access" memory (RAM). ER.II 246-251, 263-265 (declaration of FBI Agent John Powers), 279-281; ER-S.V 762-64. Volatile data is routinely overwritten or deleted over time,

and it is erased entirely whenever the computer is turned off. *Id*.; ER-S.V 762 and 764 at ¶ 10. None of this was explained in Shook's affidavit. *See* ER.II 182-84.

Shook's affidavit alleged that he has specialized training in investigating Internet and computer offenses, and that he had consulted with other agents involved in the Playpen investigation. ER-S.V 1020-21, 1022 at ¶ 6. Nevertheless, his affidavit did not disclose Tor's disc avoidance security features, even though a section of the affidavit is devoted to describing Tor. ER-S.V 1028-30 at ¶¶ 9-12.

The affidavit went on to state that the FBI sent an NIT to the "candygirl123" computer while it was connected to Playpen. ER-S.V 1035 at ¶ 28. Based on data the NIT seized from that computer, agents learned that Mr. Tippens was the internet service account holder at a residence in Hawaii. ER-S.V 1037 at ¶¶ 35-37. At the time, Mr. Tippens was serving in the Army and living in Honolulu with his mother and his two minor children. *Id*.

The investigation was largely inactive for the next six months. In September 2015, the Chief Legal Counsel for the FBI's Hawaii Field Office determined "any legal inferences we can make about SFC Tippens viewing, downloading or manufacturing child pornography is extremely low and tenuous at best." ER.II 287-90; ER-S.V 798. Consistent with this conclusion, the FBI rejected the Army's offer to postpone Mr. Tippens's pending transfer to Washington and seek a warrant to search his property while it was still in Hawaii. *Id*.; *see also* ER.II 272-73.

Mr. Tippens moved to Washington in September 2015. ER-S.V 787 at ¶ 38. That October the FBI obtained a copy of his moving inventory, which listed "valuable" and electronic items, such as a camera and printer, but did not list a computer or digital storage devices. ER.II 285-87; ER-S.V 800-14. Shook later conceded that his application contains no information showing that Mr. Tippens moved a computer from Hawaii or had one at his Washington home, such as an internet service account for the new residence. ER.II 196-200. Apart from confirming Mr. Tippens's transfer and new address in Washington, the Washington affidavit contains no information about him or his activities between the time of the Playpen visits in February 2015, and the warrant application a year later.

The application does state that "David Tippens *or another person*" residing at the Hawaii residence had connected with Playpen and there was probable cause to believe either "Tippens *or another individual*" had accessed child pornography in February 2015. ER-S.V 1027-28 at ¶ 8 (emphasis added). The application also noted that another adult (Mr. Tippens's mother) had been living at the "candygirl123" address in Hawaii and was not living at the Washington house. ER-S.V 1037-38. Shook later testified that prior to the search it was equally likely that either of the two adults who had been living at the Hawaii house was "candygirl123" and had visited Playpen. ER.II 212-14.

Nevertheless, the investigation focused exclusively on Mr. Tippens, with the Washington affidavit alleging that he fit the profile of a pornography "collector." The profile contains no individualized facts about Mr. Tippens. It nevertheless states that collectors "typically retain pictures, films, photographs . . . child erotica, and videotapes for many years." ER-S.V 1039 at ¶ 43(c). The "collector profile" also states that people who access child pornography "may" collect images; "often" maintain digital collections, "usually" at the collector's home; "may" correspond with others; and "rarely" destroy their correspondence. ER-S.V 1038-40. Det. Shook later testified that the profile was "boilerplate." ER.II 216.

In February 2016, FBI agents executed the Washington warrant at Mr. Tippens's home and seized, among other items, his personal computer. Mr. Tippens cooperated with the agents and admitted collecting pornography over many years. Ultimately thousands of pornographic pictures and videos were found on his computer, much of it child pornography, including sadistic images of very young children.

### E. MR. TIPPENS'S MOTION TO DISMISS THE INDICTMENT

Appellant moved to dismiss the indictment based on outrageous governmental conduct. ER.III 503-09; ER.IV 656-78, 717-30. The court below found "[i]t is easy to conclude that the Government acted outrageously here" and made the following specific findings:

> (1) The Government ignored the statute forbidding such conduct: "In any criminal proceeding, any property or material that constitutes child pornography ... shall remain in the care, custody and control of either the Government or the Court."18 U.S.C § 3509(m).
>
> (2) The Government facilitated the continued availability of Website A,[9] a site containing hundreds of child pornographic images for criminal users around the world.
>
> (3) The Government, in fact, improved Website A's technical functionality
>
> (4) The Government re-victimized hundreds of children by keeping Website A online.
>
> (5) The Government used the child victims as bait to apprehend viewers of child pornography without informing the victims and without the victims' permission-or that of their families.
>
> (6) The Government's actions placed any lawyer involved in jeopardy for violating ABA Model Rules of Professional Conduct 8.4, and raise serious ethical and moral issues for counsel. *See also,* Washington Rules of Professional Conduct 8.4.

ER.I 43.

Despite its misconduct findings, the court denied the dismissal motion. The court concluded that dismissal is reserved for "extreme cases in which the defendant can demonstrate that the government's conduct violates fundamental fairness" and that this is "an extremely high standard to meet." ER.I 44 (quoting *United States v. Black*, 733 F.3d 294, 302 (9th Cir. 2013)). The court determined

[9] The court referred to Playpen as "Website A," as it was originally identified in the Complaint and Government pleadings.

dismissal was unwarranted because, *inter alia*, "the Government had no individualized suspicion of any defendant"; it "created an opportunity for others to commit the crimes charged, but did not create the crimes charged"; and it "did not encourage the crimes charged-only provided the opportunity to persons unknown." ER.I 45.

### F. THE FIRST MOTION TO SUPPRESS EVIDENCE

Mr. Tippens moved to suppress all fruits of the Virginia warrant and NIT search of his computer; the court below held hearings on this and other motions in October and November 2016. ER.IV 615-639, 679-712; *see also* ER.III 309-501 (hearing transcripts).

Mr. Tippens first argued that the Virginia warrant authorized searches of persons and places only in the Eastern District of Virginia and the FBI's execution of the NIT warrant in Hawaii violated the scope of the authorization. The court did not address this issue in its order on Mr. Tippens's motions. *See* ER.I 36-64.

Appellant further argued that if the warrant could somehow be construed to authorize searches outside the district in which it was issued, as the Government maintained, then the warrant and NIT searches violated 28 U.S.C. § 636 (The Magistrate Judges Act) and Fed. R. Crim. P. 41(b). This Court has held that suppression is required when a violation of Rule 41 is deliberate, prejudicial or of constitutional magnitude. *United States v. Weiland*, 420 F.3d 1062, 1071 (9th Cir.

2005). The Court has also held that a defendant is prejudiced by a search in violation of Rule 41 if "the search would not have occurred or would not have been so abrasive if law enforcement had followed the Rule." *Id.* Appellant argued below that the Hawaii computer search plainly would not have occurred if the Rule had been followed, and also that the rule violation was deliberate and of constitutional magnitude.

The District Court concluded that, under the plain language of Rule 41, the FBI's NIT search of Mr. Tippens's computer in Hawaii had violated the Rule. ER.I 48. Nevertheless, the court ruled that the violation was "technical," not prejudicial, deliberate or "fundamental," and suppression was not required. ER.I 49-51.

Appellant's third argument regarding the Virginia warrant was that its supporting affidavit falsely claimed that Playpen displayed explicit pictures of young children on its homepage and otherwise advertised itself as a child pornography site. Further, without this false information, there was no probable cause to search every computer that merely accessed the site. ER.IV 705-10. The court below rejected these arguments, concluding that the site's appearance was "immaterial" and the warrant application "provided sufficient detail to conclude that [Playpen] was an illegal child pornography site." ER.I 46.

### G. THE SECOND MOTION TO SUPPRESS EVIDENCE

In January 2017, Mr. Tippens moved to suppress all fruits of the Washington warrant to search his home and personal computer and also moved for a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978). ER.II 269-94; *see also* ER.II 245-68, 109-243 (hearing transcript). Appellant argued that the warrant's supporting affidavit falsely stated that the "candygirl123" computer had stored copies of Playpen pictures on its hard drive. Appellant further argued that the Washington application contained a foundationless and misleading collector profile that was material to establishing probable cause to believe that evidence related to the 2015 "candygirl123" site visits in Hawaii would be found a year later in Washington. Without the collector profile, all that remained in Shook's affidavit to establish a nexus between Hawaii, where "candygirl123" had connected to Playpen, and Mr. Tippens's Washington residence were false allegations that Playpen images had been copied into long term storage on the viewer's computer and an unsubstantiated assumption that Mr. Tippens still had that computer.

The District Court denied the motions, concluding that "Detective Shook's credibility is the key to considering" Appellant's challenges. ER.I 26. The court found that Shook "did not make statements that were intentionally misleading, false or made with reckless disregard." Instead, "he relied on information from others including technical representations." *Id.* The District Court also credited

Shook's "theory" that there was "a fair probability" of finding "trace evidence" of candygirl123's viewing activity, even though this theory was not explained in his affidavit. ER.I 27. The court noted that "the theory was not airtight, but [it] cannot be said that it is based on false or misleading information." *Id.* The court reached this conclusion even though Shook's theory was contradicted by the declarations from both defense and prosecution experts. *See* ER.II 246-251, 264-265, 279-78; ER-S.V 762-64.

The court further concluded that Shook's theory was "strengthened in light of the collector profile." ER.I 27. The court found that "[g]iven Detective Shook's broad understanding of downloading and viewing as equivalent and his belief that viewing leaves trace files of evidentiary value on a user's computer, including Tor users, in a strict sense, a downloader (and thus a viewer) also possesses and receives, which satisfied the foundation for the collector profile." ER.I 28-29. The court also found it significant that "candygirl123" had been logged into Playpen for a total of 26 hours and the site required "some sophistication" to locate. ER.I 28.

The court concluded that the challenges to Shook's affidavit "should give the FBI pause about some of its investigatory practices and assumptions about offenders' characteristics." ER.I 34. The court warned that "[v]igilance must persist to ensure that we do not 'let the nature of the crime, child pornography,

skew our analysis or make us 'lax' in our duty to guard the privacy protected by the Fourth Amendment.'" *Id*. (quoting *United States* v. *Gourde*, 440 F.3d 1065, 1075 (9th Cir. 2006)).

### H. THE TRIAL AND SENTENCING

A bench trial was held before The Hon. Robert J. Bryan on March 13-15, 2017. At the end of the prosecution's case, the court granted a defense motion to dismiss the receipt and transportation counts (Counts One and Three of the Superseding Indictment). ER.I 18. The dismissals were based on the Government's refusal to disclose the NIT components and its efforts to prevent the defense from introducing government documents that undermined the prosecution's claims that the NIT did not alter or corrupt evidentiary data. ER.I 13-15. The court also found that the prosecution was withholding information that would have enabled the defense "to attack the Government's credibility as to representations made at *ex parte* and *in camera* [classified information] hearings" that had previously been held in connection with defense motions to compel discovery. ER.I 15.

Mr. Tippens did not contest the remaining possession count and the court found him guilty of that charge. ER.I 15. Mr. Tippens was later sentenced to six months in custody and ten years of supervised release. ER.I 4-5. During sentencing the court observed that "I don't know that I have seen a case where there was more clear acceptance of responsibility than this one." ER.II 98. Mr. Tippens cooperated

with the police, "immediately disclosed his guilt," and did not contest at trial the offense for which he was convicted. *Id*. While recognizing that Mr. Tippens had committed "a very serious offense," ER.II 99, the court concluded that "he is essentially a very good person, a good citizen, that has done a bad thing." ER.II 101. The court noted Mr. Tippens was a decorated veteran (he earned a Bronze Star, among other medals, for his service in Iraq); he struggled with Post Traumatic Stress Disorder and depression related to his military service; he did not have a criminal record; he had fully engaged with counseling; and he had had perfect compliance with pretrial supervision. The court also found that "he has by all accounts been not only an adequate but outstanding parent to his two daughters, and he protected them from his activities that were inappropriate." ER.II 100-101.

## VIII. ARGUMENT

### A. THE GOVERNMENT'S GLOBAL DISTRIBUTION OF CHILD PORNOGRAPHY WAS OUTRAGEOUS CONDUCT WARRANTING DISMISSAL OF THE INDICTMENT

The Government's unprecedented conduct in this case was outrageous and requires dismissal under this Court's supervisory powers and the due process clause. *See United States v. Ross*, 372 F.3d 1097, 1109 (9th Cir. 2004), *on rehearing in part*, 138 Fed. App'x 902 (2006). "A court may exercise its supervisory powers to dismiss an indictment in response to outrageous government conduct that falls short of a due process violation." *Id*.

### 1. The Government's outrageous conduct irreparably harmed victims and their families

The degree of harm the Government caused cannot be overstated. The Government itself has emphasized the harms minor victims may experience from online distribution of their images. For example, DOJ's website states the following:

> [V]ictims of child pornography suffer not just from the sexual abuse inflicted upon them to produce child pornography, but also from knowing that their images can be traded and viewed by others worldwide. *Once an image is on the Internet, it is irretrievable and can continue to circulate forever.* The permanent record of a child's sexual abuse can alter his or her live (*sic*) forever. Many victims of child pornography suffer from feelings of helplessness, fear, humiliation, and lack of control given that their images are available for others to view in perpetuity.[10]

(Emphasis added); *see also*, *e.g.*, DOJ Press Release, Ellettsville Man Charged with Production of Child Pornography, April 15, 2015 ("Producing and distributing child pornography re-victimizes our children every time it is passed from one person to another)."[11]

The Supreme Court has endorsed the Government's view of these harms and explained that circulating child pornography "renew[s] the victim's trauma" and

---

[10] Available at: http://www.justice.gov/criminal-ceos/child-pornography. This statement appears as part of the mission statement for the Child Exploitation and Obscenity Section (CEOS), which helped supervise the Playpen operation.

[11] Available at: http://www.justice.gov/usao-sdin/pr/ellettsville-man-charged-production-child-pornography.

makes it difficult for victims to recover from abuse." *Paroline v. United States*, 134 S. Ct. 1710, 1717 (2014). Moreover, the Government routinely (and unsurprisingly) maintains that the administrators of child pornography sites are far more culpable than people who simply view or collect pornography, because site operators make pornography available to far more people. ER.IV 724.

The Government's misconduct was not only callous but unjustifiable, because there was no investigatory need to maintain Playpen as a "fully operational" site. That is because the Virginia warrant authorized the FBI to deploy its NITs while visitors were still logging in and before they accessed the site's contents or posted new images.

In addition, even if the Government needed to maintain the credibility of the site to avoid "tipping off" visitors, there were a variety of ways it could have done that while at least limiting the torrent of pornography that flowed from Playpen (a fact it did not dispute). *See* ER.III 506-07. For example, the Government could have edited the contents of the site to include only child erotica or virtual pornography; removed all forums with the most egregious content; blocked directories and links with "error" messages, which were common to Playpen and other Tor sites anyway; or used a "spoofing" system, where visitors to Playpen were secretly redirected to a facsimile of the site, minus any content or links that agents did not want accessible. *Id*.; ER.III 506-07, 526-30; ER.IV 656-59, 661-64,

668-69, 725-26; *see also* Corey Young, FBI Allowed for More Victimization by Permitting a Child Pornography Website, The New York Times, January 27, 2016 (discussing investigatory alternatives to the "immoral and inexcusable" Playpen operation).[12]

Instead of doing any of those things, the FBI actually improved the speed and accessibility of Playpen, and even upgraded the file hosting features that enabled visitors to upload and download content. ER.I 43 (misconduct finding (3)); *see also* ER-S.V 941 at ¶ 24 (explaining file hosting); ER.III 527-28; ER.IV 676 (user comment that "Clearly PlayPen runs considerably faster and more stable now. Thanks a lot keep it up PP crew!").

### 2. The Government's disregard for a previous judicial reprimand warrants dismissal now to deter future misconduct

Dismissal here is not only appropriate but necessary to deter similar misconduct in the future. A court's broad supervisory power to dismiss an indictment for misconduct "may be exercised for three reasons: to remedy a constitutional or statutory violation; to protect judicial integrity by ensuring that a conviction rests on appropriate considerations validly before a jury; or to deter future illegal conduct." *United States v. Barrera-Moreno*, 951 F.2d 1089, 1091

[12] Available at: http://www.nytimes.com/roomfordebate/2016/01/27/the-ethics-of-a-child-pornography-sting/fbi-allowed-for-more-victimization-by-permitting-a-child-pornography-website.

(9th Cir. 1991). In this case, the court below found that the Government had violated the law by wantonly distributing child pornography and also placed itself in ethical "jeopardy," and this Court should conclude that dismissal is the only effective means of deterring similar future conduct.

Significantly, this is not the first time the Government has been reprimanded for distributing child pornography and victimizing children. Over a decade ago, the Seventh Circuit expressed outrage at the Government's uncontrolled delivery of child pornography. *United States v. Sherman*, 268 F.3d 539 (7th Cir. 2001). In *Sherman*, federal agents supplied the defendant "with a literal catalog of child pornography, and then delivered to him materials that depicted actual children, allowing him enough time to view and even copy the materials before arresting him." *Id*. at 548.

The Government justified its methods on the ground that its "larger purpose" was to prevent future crimes. *Id.* at 548-49. The court was unpersuaded and, even though Sherman had not raised an outrageous conduct challenge, *sua sponte* rebuked the Government because its "participation in criminal activity in the course of an investigation should rarely, if ever, involve harming actual, innocent victims." *Id.* at 549.

> We are aware of the necessity of such tactics in so-called victimless crimes such as drug offenses, but the use of these methods when victims are actually harmed is inexplicable. 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.

*Id.*

The court also cautioned the Government that "its investigative technique in this case was inconsistent with its position . . . that the children depicted are harmed by the continued existence of and mere possession of child pornography." *Id*. at 550. While recognizing that investigating pornography offenses can be difficult, the Seventh Circuit concluded that "[w]e have no doubt that creative investigative techniques and tight controls on the materials used as bait for the consumers of child pornography can lead to better protection of the victims of child pornography." *Id*.

Yet, here, DOJ and the FBI ignored the court's admonition, imposing *no protocols whatsoever* for its handling or containment of the child pornography on Playpen. ER.III 527-30 (testimony of Lead Agent Alfin). This is true even though Operation Pacifier was supervised by senior DOJ and FBI personnel and some of the concerns spelled out in *Sherman* have been incorporated into DOJ's own "Online Investigative Principles." *Id.*; ER.III 515-17; ER.IV 727-29; DOJ, Online Investigative Principles for Federal Law Enforcement Agents.[13]Among other

[13] Available at: https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf.

relevant warnings, the Investigative Principles caution attorneys and agents about the harms that can arise from online investigations:

> [O]nline undercover facilities that offer the public access to information or computer programs that may be used for illegal or harmful purposes may have greater capacity than similar physical-world undercover entities to cause unintended harm to unknown third parties. *Because digital information can be easily copied and communicated, it is difficult to control distribution in an online operation and so limit the harm that may arise from the operation.*

*Id*. at 44 (p. 57 of the PDF) (emphasis added); *see also id*. at 45 (p. 58 of PDF) (explaining that undercover online facilities are likely automated and contraband on them can be "endlessly replicated and distributed to others" resulting in harm "to innocent third parties").

Because the Government ignored the disapproval of the Seventh Circuit, the trial court's admonishments in this case will not deter future similar misconduct. Given the explicit findings of outrageous conduct and the undisputed facts below, as well the Government's failure to heed prior judicial warnings, this Court should now sanction the Government as a necessary deterrent to similar misconduct in the future. Appellant further submits that dismissal of the indictment or, at this stage, reversal of his conviction are the only effective sanctions.

### 3. The Government's outrageous conduct violated due process and requires dismissal of the indictment

Although this Court should dismiss the indictment under its supervisory powers, the extent of the Government's misconduct warrants dismissal as a matter

of due process. The Supreme Court has long held that the federal judiciary has the power to evaluate a criminal case's entire proceedings to determine whether they "offend those canons of decency and fairness which express the notions of justice of English-speaking peoples even toward those charged with the most heinous offenses.'" *Rochin v. California*, 342 U.S. 165, 169 (1952) (quoting *Malinski v. New York*, 324 U.S. 401, 416-17 (1945)). When the Government violates these standards of "decency and fairness," due process concerns are implicated. *See id*. Hence, governmental conduct that "shocks the conscience" may constitute a due process violation, requiring dismissal. *Rochin* at 172.

Government conduct that offends due process to a degree warranting dismissal is rare and the threshold for dismissal is "extremely high[.]" *United States v. Smith*, 924 F.2d 889, 897 (9th Cir. 1991). At the same time, there is no "formalistic checklist" for determining whether "law enforcement conduct crosses the line between acceptable and outrageous" and "every case must be resolved on its own particular facts" in light of the "totality of circumstances[.]" *United States v. Black*, 733 F.3d 294, 302, 304 (9th Cir. 2013). This Court should find that the totality of the unprecedented circumstances in this case warrants dismissal.

### B. THE SEARCH OF MR. TIPPENS'S HAWAII COMPUTER WAS NOT AUTHORIZED BY THE VIRGINIA WARRANT

If the Court does not dismiss the indictment, then it should order suppression of all fruits of the NIT search of Mr. Tippens's computer in Hawaii because the

Virginia warrant only authorized searches of "person[s] or property located in the Eastern District of Virginia." ER-S.V 922, 954.

To state the obvious, a warrant that authorizes searches in one location does not authorize searches in another location. *See, e.g., Hunt v. Tomplait*, 301 F. App'x 355, 356 (5th Cir. 2008) (warrant issued for 126 Circle Drive did not justify search of 940 Church Street; affirming denial of qualified immunity for officers involved in search); *Simmons v. City of Paris, Tex.*, 378 F.3d 476 (5th Cir. 2004) (warrant for 400 N.W. 14th Street did not justify search of 410 N.W. 14th Street; affirming denial of qualified immunity for officers involved in search).

In addition, the Supreme Court has held that if the scope of a search exceeds that permitted by a warrant's express terms, then any seizure during the search is unconstitutional and nothing more need be shown for suppression. *Horton v. California*, 496 U.S. 128, 140 (1990); *see also United States v. Sedaghaty*, 728 F.3d 885, 915 (9th Cir 2013) ("[T]he exclusionary rule generally bars admission of the evidence seized that was beyond the scope of the warrant.").

In this case, the Virginia warrant specified "the Eastern District of Virginia" as the place where authorized targets of the NIT searches are located. ER-S.V 954. It then referred to its "Attachment A" to further "identify the person or describe the property to be searched and give its location." *Id*. Attachment A, captioned "Place to be Searched," states the NIT will be used for "[o]btaining information... from

the activating computers described below." ER-S.V 955. "Activating computers" are "those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password." *Id*. The "Target Website" is Playpen, which was already under the control of the FBI.

The warrant and Attachment A therefore authorized the FBI to search any "activating computers" located in the Eastern District of Virginia that connected with Playpen. Accordingly, the search of Mr. Tippens's Hawaii computer violated the scope of the warrant and the fruits of that search should be suppressed.

This conclusion is not altered by the language on page 29 of the warrant application referencing computers "wherever located." ER-S.V 951. "It is the description in the search warrant, not the language of the affidavit, which determines the place to be searched." *Sedaghaty*, 728 F.3d at 914. In *Sedaghaty*, the Court was evaluating whether the items seized were particularly described in the warrant, rather than whether the location was properly described. However, the Court made clear that these particularity requirements apply equally to a description of the search location. *Id*. at 914. Thus, language in a warrant application cannot alter the scope of a warrant.

The only exception to this bright line rule is a narrow one and inapplicable here. In *United States v. SDI Future Health, Inc.*, 568 F.3d 684 (9th Cir. 2009), the Court held that "[w]e consider an affidavit to be part of a warrant, and therefore

potentially curative of any defects, *only if* (1) the warrant expressly incorporated the affidavit by reference *and* (2) the affidavit either is attached physically to the warrant or at least accompanies the warrant while agents execute the search." *Id.* at 699 (emphasis added; internal quotation marks and citation omitted). In this case, the warrant did not expressly incorporate the affidavit, and the affidavit was neither attached to the warrant nor did it accompany it during execution.

In short, the Virginia warrant is limited on its face to the Eastern District of Virginia. The Court should therefore reject any effort by the Government to "reverse engineer" the warrant and should order all fruits of the NIT search suppressed.

### C. IF INTENDED TO BE A GLOBAL WARRANT, THE WARRANT VIOLATED RULE 41, REQUIRING SUPPRESSION

#### 1. The court below correctly concluded that Rule 41 did not allow the Government to use the Virginia warrant to search Appellant's computer

If the Court finds that the Virginia warrant was not limited on its face to the Eastern District of Virginia, it should find that the warrant exceeded the issuing judge's authority under Rule 41. A magistrate judge's authority to issue warrants is limited by 28 U.S.C. § 636 and Fed. R. Crim. P. 41. At the time the NIT warrant was issued, magistrate judges had no authority to issue warrants for searches outside their judicial districts, except in terrorism cases. As a result, even if the

NIT warrant purported to authorize searches anywhere in the world, it was incapable by law of doing so and suppression is still required.

Pursuant to 28 U.S.C. § 636(a), magistrate judges have jurisdiction "within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law," including Rule 41. *See generally Dawson v. Marshall*, 561 F.3d 930, 932 (9th Cir. 2009) ("Section 636 outlines the jurisdiction, powers, and temporary assignments of magistrate judges."). At the time, Rule 41(b) authorized warrants in five different situations: 1) for "a person or property located within the district"; 2) for a person or property "outside the district if the person or property is located within the district when the warrant is issued"; 3) "in an investigation of domestic terrorism or international terrorism"; 4) to install within the district a "tracking device"; and 5) "for property that is located outside the jurisdiction of any state or district, but within . . . a United States territory, possession, or commonwealth" and other locations not relevant here.[14] As is virtually self-evident and the court below correctly concluded, none of these provisions allowed a Virginia judge to issue a warrant for a Hawaii computer in a non-terrorism case. ER.I 48.

[14] Rule 41 was later amended, effective December 1, 2016. Subsection (b)(6) of the amendment now authorizes magistrate judges, *inter alia*, to issue warrants for "remote access" searches outside their districts to seize data when it "has been concealed through technological means."

Not only did the magistrate judge in this case lack authority to issue a global warrant but, as the previous section makes clear, she evinced no intention to do so. "Trial judges are presumed to know the law and to apply it in making their decisions." *Clark v. Arnold*, 769 F.3d 711, 727 (9th Cir. 2014) (quoting *Walton v. Arizona*, 497 U.S. 639, 653 (1990)), *overruled on other grounds by Ring v. Arizona*, 536 U.S. 584 (2002). There is no reason to believe the magistrate here intended to issue an unprecedented worldwide warrant without her making that intention clear by amending the warrant's description of the location to be searched. This Court should therefore conclude that the judge who issued the Virginia warrant was fully aware of the limits of her jurisdiction and, consistent with her authority, only authorized searches for computers in Eastern Virginia.

**2. Suppression is required for the Rule 41 violation**

If the Court finds that the Virginia magistrate issued a global warrant, it exceeded the magistrate's legal authority and was invalid. This Court has explained that "[f]ederal magistrates are creatures of statute, and so is their jurisdiction. We cannot augment it; we cannot ask them to do something Congress has not authorized them to do." *United States v. Colacurcio*, 84 F.3d 326, 328 (9th Cir. 1996) (citation omitted). Hence, if a magistrate issues a warrant she has no authority to issue, that violation cannot be excused as a mere "technical" defect and the warrant is invalid, rendering a search pursuant to it effectively warrantless.

*United States v. Glover*, 736 F.3d 509, 515 (D.C. Cir. 2014) (the language of Rule 41(b) is "crystal clear" and a "jurisdictional flaw" in the warrant cannot be excused as a "technical defect."); *see also United States v. Barber*, 184 F. Supp. 3d 1013, 1018 (D. Kan. 2016) (warrant was issued by a Maryland magistrate judge for digital evidence in California; the court concluded "warrants issued without jurisdiction are void from their inception"); *cf. Allen v. Meyer*, 755 F.3d 866, 867 (9th Cir. 2014) ("Because the magistrate judge entered judgment [outside the limits of § 636], the judgment was invalid."); *United States v. Scott*, 260 F.3d 512, 515 (6th Cir. 2001) (holding that "when a warrant is signed by someone who lacks the legal authority necessary to issue search warrants, the warrant is void ab initio"), *overruled on other grounds*, *United States v. Master*, 614 F.3d 236, 242 (6th Cir. 2010).

A violation of Rule 41 in this case would require suppression. Suppression of evidence obtained through a search that violates Rule 41 is required if one of three things occurs:

> 1) the violation rises to a constitutional magnitude; 2) the defendant was prejudiced, in the sense that the search would not have occurred or would not have been so abrasive if law enforcement had followed the Rule; or 3) officers acted in 'intentional and deliberate disregard' of a provision in the Rule.

*United States v. Weiland*, 420 F.3d 1062, 1071 (9th Cir. 2005) (citations omitted). Here, the Government achieved a trifecta, because its NIT search was not only prejudicial, but also deliberate and of constitutional magnitude.

**a. Appellant was prejudiced by the search of his computer**

Mr. Tippens was "prejudiced" under *Weiland* because the search of his computer "would not have occurred" if the warrant and search had complied with Rule 41(b). Simply put, since Rule 41 did not allow the FBI to use a Virginia warrant to search a Hawaii computer, that search would not have occurred if the Government had followed the Rule.

The court below, however, concluded that this "interpretation" of *Weiland* would mean that "all searches executed on the basis of warrants in violation of Rule 41(b) would result in prejudice, no matter how small or technical the error might be," and this is not a "workable interpretation." ER.I 50. The court instead created its own standard: "whether evidence obtained from a warrant that violates Rule 41(b) could have been available by other lawful means, and if so, the defendant did not suffer prejudice." *Id*. The court then concluded that Mr. Tippens "did not suffer prejudice when [he] revealed to a third party the identifying information, [his] IP address[], to which [he] had no reasonable expectation of privacy." *Id*. The court's analysis and legal conclusions were erroneous for several reasons.

First, by no means can all violations of Rule 41 be considered prejudicial if this Court affirms *Weiland*'s straightforward definition of prejudice, rather than the District Court's definition. For example, in a case decided the year after *Weiland*, this Court held a police officer's failure to provide a copy of the warrant he was executing to a person on the premises was a technical violation of Rule 41 not requiring suppression. *United States v. Williamson*, 439 F.3d 1125 (9th Cir. 2006). The defendant conceded, and the Court held, that there was no prejudice, because the search would still have occurred if the Rule had been followed.

By contrast, a judge who issues a warrant she has no authority to issue commits more than a technical violation, and any searches undertaken pursuant to the warrant prejudice the defendant under *Weiland*. *Compare Williamson*, *supra*, with *United States v. Krueger*, 998 F. Supp. 2d 1032 (D. Kan. 2014) (suppressing where Government obtained warrant in Kansas for a house in Oklahoma because "defendant has shown prejudice in that if Rule 41(b)(2) 'had been followed to the letter'" the warrant would not have issued). To characterize "prejudice" in the way the court below did would effectively overrule *Weiland* and allow both judges and law enforcement officers to ignore the requirements of Rule 41 with impunity, even though those requirements "have the force of statute." *Hilao v. Estate of Marcos*, 95 F.3d 848, 852 (9th Cir. 1996).

The court below also erred when it concluded Appellant was not prejudiced by the NIT search, on the theory he had no reasonable expectation of privacy in his IP address because those addresses are typically shared with third parties, such as internet service providers. ER.I 50-51. This conclusion ignores the fact that the NIT did not just seize an IP address. It also seized other identifying data which was not shared with third parties, such as Mr. Tippens's MAC address and the usernames stored in his operating system. *See, e.g.*, ER-S.V 948 at ¶ 26.

The court also overlooked the fact that the Virginia warrant application itself stated that "traditional IP identification techniques are not viable" and that "[t]here is no practical way to trace the user's actual IP back" through the Tor network. ER.I 11 at ¶ 8; *see also* ER.I 12 at ¶ 9, 22 at ¶ 29. Since the reason people use Tor is to keep their IP addresses and other identifying data private, and Tor is known to be an effective tool for doing that, it makes sense to conclude that Tor users have a reasonable expectation of privacy when they are using the network. As another district court explained when ordering suppression following an NIT search, "[w]ere the IP address obtained from a third-party, the Court might have sympathy" for the Government's position that the defendant had no privacy interest in the address. *United States v. Arterbury*, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091 at *35, (N.D. Okla., Apr. 25, 2016).

> However, here the IP address was obtained through use of computer malware that entered Defendant's home, seized his computer and

> directed it to provide information that the [Virginia] affidavit states was unobtainable in any other way. Defendant endeavored to maintain the confidentiality of his IP address, and had an expectation that the Government would not surreptitiously enter his home and secure the information from his computer.

*Id.* at *30.

Moreover, because the NIT search in this case was of Mr. Tippens's personal computer located in his home, the search implicated core privacy interests regardless of what was seized or whether it was shared. "The sanctity of a person's home, perhaps our last real retreat in this technological age, lies at the very core of the rights which animate the [fourth] amendment." *United States v. Becker*, 23 F.3d 1537, 1539 (9th Cir.1994) (citation omitted). In addition, the "Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained" during a residential search. *Kyllo v. United States*, 533 U.S. 27, 37 (2001). Finally, because the NIT search was of Mr. Tippens's personal computer, it makes no difference for Fourth Amendment purposes whether some of the evidence seized during that search was obtainable elsewhere. *Cf. Riley v. California*, 134 S. Ct. 2473, 2490-91 (2014) (defendant had privacy interest in data stored on his cell phone, regardless of whether some or all of that data was also stored with third parties).

In short, the court below erred in concluding that Mr. Tippens was not prejudiced by the NIT search and also concluding that the search did not implicate a reasonable expectation of privacy.

**b. Suppression is also required because the violation of Rule 41 was deliberate**

This Court also requires suppression of evidence if officers acted in "intentional and deliberate disregard" of Rule 41, regardless of whether there is a showing of prejudice. *Weiland*, 420 F.3d at 1071 (citations omitted); *see also United States v. Martinez-Garcia*, 397 F.3d 1205, 1213 (9th Cir. 2005) (same). Apart from the fact that there is no credible interpretation of Rule 41 that would allow for a global hacking warrant, three additional facts establish that the Government deliberately violated the rule: 1) the Government was denied an NIT warrant in 2013 when the location of the target computer was unknown; 2) beginning later that year the Government sought to amend Rule 41 to make such searches legal; and 3) the Government's own analysis of Rule 41 reveals that it fully understood the Rule's prohibition of multi-jurisdictional warrants.

In 2013, a federal court denied an application for an NIT warrant in a fraud case because the location of the target computer was unknown and issuing the warrant would have violated Rule 41. *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013) ("*In re Warrant*"). This is the only known published opinion addressing the legality of an NIT warrant

prior to Operation Pacifier. As in the instant case, the Government sought a warrant to send malware to a computer in an unknown location to seize its IP address and other data. *Id*. at 755. The court analyzed the Rule and concluded its plain language precluded the type of warrant the Government sought. The court then noted that "there may well be a good reason to update the territorial limits of [Rule 41] in light of advancing computer search technology," but until then it had no authority to issue the warrant. *Id*. at 760.

With this case in mind, the Government began seeking amendments to Rule 41 that did not go into effect until December, 2016. In fact, DOJ cited *In re Warrant* in its correspondence with the Advisory Committee on the Criminal Rules as one of the reasons for amendment. ER.IV 699; ER-S.VI 1085. This letter shows that DOJ was fully aware, at least two years before it sought the NIT warrant here, that Rule 41 did not permit multi-district computer hacking warrants. *See also* ER-S.VI 1086 (where DOJ stated that the Rule should be changed to "remove an unnecessary *obstruction currently impairing* the ability of law enforcement to investigate . . . multi-district Internet crimes") (emphasis added).

The deliberate nature of the Rule violation in this case is further evidenced by DOJ's own computer search guidelines and analysis of Rule 41, which reached conclusions similar to those of the *In re Warrant* court. According to DOJ, "[a]gents should obtain multiple warrants if they have reason to believe that a

network search will retrieve data stored in multiple locations." DOJ, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations at 84 (issued January 14, 2015).[15] DOJ's guidelines go on to state that when "data is stored remotely in two or more different places within the United States and its territories, *agents should obtain additional warrants for each location where the data resides to ensure compliance with a strict reading of Rule 41(a).* For example, if the data is stored in two different districts, agents should obtain separate warrants from the two districts." *Id*. at 84-85 (emphasis added). The guidelines also address situations where, as here, "agents do not and even cannot know that data searched from one district is actually located outside the district[.]" *Id*. at 85. In these situations, the manual explained that agents will be inviting suppression if they disregard the Rule's jurisdictional limits. *Id*.

Given the plain language of Rule 41, the *In re Warrant* decision, and DOJ's own guidelines, the Government cannot credibly maintain it unwittingly ran afoul of the Rule in this case. And, like the *In re Warrant* court, the court below found that construing the provisions of Rule 41 to allow for global NIT searches would "stretch their language far beyond their intent," even "when flexibly applying the rule." ER.I 48.

[15] Available at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

Nevertheless, the District Court found that the Government did not deliberately violate the Rule. Focusing on DOJ's efforts to amend the Rule while simultaneously doing the very things only allowed after an amendment, the court concluded that this inconsistency could be explained as merely an "intent to improve the rule, which does not rule out the possibility that DOJ could have considered Rule 41(b) sufficiently flexible to address changes in technology." ER.I 15.

This conclusion, however, does not make sense and has no support in the record. The Government did not offer testimony or other evidence from DOJ personnel involved in the amendment process or anyone who had approved the Virginia warrant application. It also refused to provide the defense with discovery related to its approval of the application and oversight of Operation Pacifier. ER-S.V 919-20. Most basically, however, the District Court's speculation about the Government's intentions is at odds with its conclusion that there is no legitimate way to construe Rule 41 that would have allowed the NIT searches. As a matter of common sense, if someone knows a rule and there is no credible way to interpret it that would allow that person to do what she did, then it is safe to conclude that her violation of the rule was deliberate. *See also United States v. Coreas*, 419 F.3d 151, 151 (2d Cir. 2005) ("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. If they do so, however, they endanger the freedom of all of us.").

In short, this Court should find that the Government deliberately violated Rule 41 in this case. Suppression is the required remedy for a deliberate violation, even if a defendant has not been prejudiced by it. *See also United States v. Gantt*, 194 F.3d 987, 1005 (9th Cir.1999), *overruled on other grounds by United States v. W.R. Grace*, 526 F.3d 499, 506 (9th Cir. 2008) (suppression required when agents' refusal to provide warrant to its subject was deliberate and the court not need "consider whether the violation was 'technical' or 'fundamental'"); *see also* § C(2)(a) above (establishing that Appellant was prejudiced).

**c. Suppression is also required because the violation was of constitutional magnitude**

Finally, regardless of whether a defendant is prejudiced by a search that violated Rule 41 or the violation is deliberate, this Court has held that suppression is required if the violation is of constitutional magnitude. *Weiland*, 420 F.3d at 1071. "Constitutional magnitude" is not defined in *Weiland* or elsewhere, but if the violations at issue in this case are not of constitutional magnitude, it is hard to imagine what violation would be.

According to the Government, the Virginia warrant authorized it to execute searches on a target population (approximately 100,000 visitors) so large that it is equivalent to the entire population of many small cities, such as Boulder, Colorado,

and Everett, Washington. The Government also maintains that it was a global warrant, authorizing it to search computers in 120 other countries.[16] And, according to the Government, the warrant gave it this unprecedented search and seizure power even though the warrant states that the places to be searched are within the Eastern District of Virginia, and any searches outside that jurisdiction violated Rule 41. *See generally Gomez v. United States*, 490 U.S. 858, 872 (1989) (limits on magistrate judges' authority are "circumscribed in the interests of policy as well as constitutional constraints").

All of this power that the Government is claiming, moreover, is predicated on an affidavit that contains no particularized information about any of the thousands of people targeted by the search, apart from the fact they visited a website that does not even look like a child pornography site. *See generally United States v. Vasquez*, 654 F.3d 880, 884 (9th Cir.2011) ("The prohibition of 'general warrants' imposes a particularity limitation, requiring warrants to specify the items to be seized and the locations to be searched"); *see also* Kevin Poulsen, *Visit the Wrong Website, and The FBI Could End Up in Your Computer*, Wired.com, August 5, 2014 (although use of "malware" by the FBI is not new, "[w]hat's

[16] *Compare* ER-S.V 869 (DOJ letter to Advisory Committee on Federal Rules), stating that even under the amended Rule 41 "there is a presumption against extraterritorial application" of warrants and the rule change "does not purport to authorize courts to issue warrants that authorize the search of electronic storage media located in a foreign country or countries." *See also* ER-S.V 854.

changed is the way the FBI uses its malware capability, deploying it as a driftnet instead of a fishing line.").[17]

Given these facts, the Government will be asking this Court to approve what is tantamount to a cyber-age general warrant, a result that is anathema to the protections enshrined by the Fourth Amendment. *See Ashcroft v. al-Kidd*, 563 U.S. 731, 742 (2011) ("The Fourth Amendment was a response to the English Crown's use of general warrants, which often allowed royal officials to search and seize whatever and whomever they pleased while investigating crimes"). This Court should therefore conclude that the rule violations in this case are of constitutional magnitude and warrant suppression. To hold otherwise would allow judges to issue future warrants without regard for the requirements of Rule 41 and permit law enforcement to violate those requirements when they do not suit its purpose.

### D. THE VIRGINIA WARRANT WAS BASED ON MATERIAL FALSE STATEMENTS, WITHOUT WHICH THERE WAS NO PROBABLE CAUSE TO SEARCH THOUSANDS OF COMPUTERS, INCLUDING APPELLANT'S

Probable cause in this case is inextricably linked with *Franks* issues, as the court below relied on false statements in the Virginia warrant application to find probable cause, then turned around and found the falsehoods "immaterial." ER.I 46. The application alleged that Playpen advertised itself as a child pornography

[17] Available at: http://www.wired.com/2014/08/operation_torpedo/

site and displayed explicit pictures of minors on its homepage. Neither of those assertions is true. In addition, the record establishes that the false statements were made either intentionally or recklessly. The Court should therefore excise the false statements from the application, find that probable cause is lacking without them, and suppress all fruits of the NIT search in this case. *Franks*, 438 U.S. at 163-64.

As a general matter, the Supreme Court has held "when the Fourth Amendment demands a factual showing sufficient to comprise 'probable cause,' the obvious assumption is that there will be a *truthful* showing." *Id.* (quotation marks and citation omitted; emphasis in original). Where, as here, the record establishes that an affidavit contains intentional or reckless false statements that are material to probable cause, the proper approach is "to delete false or misleading statements and insert the omitted truths revealed at the suppression hearing." *United States v. Ippolito*, 774 F.2d 1482, 1487 (9th Cir. 1985)*; see also United States v. Condo*, 782 F.2d 1502, 1506 (9th Cir. 1986) (once a *Franks* violation is established, the remedy is to review the "reformed" affidavit and make a *de novo* determination of probable cause, without the usual deference to the issuing magistrate). The doctrine also applies when the affiant included "intentionally or recklessly omitted facts required to prevent technically true statements in the affidavit from being misleading." *United States v. Stanert*, 762 F.2d 775, 781 (9th Cir.), *amended by* 769 F.2d 1410 (1995).

In this case, the court below held a *Franks* hearing based on Appellant's preliminary showing of material falsehoods in the Virginia application. The court concluded, however, that the statements at issue were "immaterial." ER 46. This conclusion was erroneous and should be reversed.

### 1. The District Court's probable cause findings were fatally based on false statements and its misunderstanding of the Tor network

The lynchpin of the District Court's finding that the affidavit established probable cause was that "[t]he FBI affiant described in detail the homepage, which featured two prepubescent, partially clothed females, as well as text instructing users how to post photos and video material." ER.I 46; *see also* ER-S.V 934-35 at ¶ 10 (where the application in fact described the homepage as displaying "images of prepubescent females partially clothed and whose legs are spread"); ER-S.V 935 at ¶ 12 (claiming that the page showed two "partially clothed prepubescent females with their legs spread"). Moreover, the tiny technical text on the page is both obscure and commonplace. *See* ER-S.V 935 ¶ 12; ER-S.VI 1105-07. For example, ".7z preferred" refers to a popular file compression format. *Id.*; *see also* http://www.makeuseof.com/tag/keka-file-compressor-for-mac; http://www.7-zip.org/7z.html.

In further support of its probable cause determination, the court found that "[t]he [Playpen] website was not publicly available and could be found only by

using a Tor hidden service," that Playpen could not be located with a Google search and users had to know the site's address, and that the FBI targeted "registered users." ER.I 46. These findings, without the false description of the homepage, do not establish probable cause.

Problematically, the district court's most facially convincing factor supporting cause, the appearance of the homepage, was not true. In fact, the homepage did not display "prepubescent girls" or any sexual images. *See* ER-S.VI 1083; *see also* ER-SVI 1100-01, 1108-10. The site also did not advertise its contents. For example, its homepage contained no references to pornography or "Lolitas," and otherwise did not show that it contained child pornography. Indeed, as Lead Agent Alfin himself admitted, the homepage displayed merely a single small picture of a young woman or older teenager, seated, clothed and unremarkable in appearance, not the pictures described in the warrant application. *See* ER-S.VI 1083. Thus, the District Court supported its probable cause finding with a statement that the Government itself conceded was not true. For these reasons, the appearance of Playpen's homepage does not support a finding of probable cause.

The other bases for the district court's probable finding reflect a misunderstanding of the Tor network and are dubious at best. Contrary to the court's finding that Playpen "was not publicly available and could be found only

by using a Tor hidden service," the site was accessible to anyone and was itself a "Tor hidden service," simply meaning that it was a Tor site. *See* ER-S.V 933-34. Moreover, there is nothing inherently suspect about Tor; it is funded by the Government and has millions of ordinary users who want "to protect their privacy from unscrupulous marketers and identity thieves," prevent corporations from collecting personal information, and exercise free speech in countries with repressive regimes.[18] As noted earlier, DOJ recommends that federal judges use Tor.

The court also concluded that Playpen could not be located with a Google search and users had to know the site's address. ER.I 46. While it is true that Google is not a Tor search engine, there are many other search engines and site "indexes" for Tor and visitors could find Playpen with these tools. *See, e.g*. Kristen Hubby, Here Are the 13 Best Deep Web Search Engines, dailydot.co (Nov. 28, 2016).[19] More importantly, Playpen's visitor traffic was enormous, with approximately 100,000 visitors in just 15 days, indicating that the site was not secret.

[18] *See* https://www.torproject.org/about/torusers.html.en. https://www.dailydot.com/layer8/best-deep-web-search-engines/

[19] Available at: https://www.dailydot.com/layer8/best-deep-web-search-engines/

Finally, the court found that the FBI only searched the computers of "registered users." ER.I 46. It is unclear what the court meant by "registered users," but the undisputed facts are that the FBI targeted all visitors (including first time visitors) while they were logging in to the site and before they could see its contents. *See, e.g.*, ER-S.V 946 at ¶ 32. In addition, the Government elected to seek the Virginia warrant without offering particularized information about any Playpen users, even though it had reams of data about them. With control of Playpen's server, the Government possessed the user names of 158,000 "members" and detailed data about their activities on the site, such as the specific pictures or videos they viewed. *See* ER-S.V 939-941, 1032-33. The FBI also had IP addresses for approximately 1000 users before the NIT searches. ER-S.V 944 at n. 7. But instead of using that information to narrow the NIT searches and target specific members, the Government sought the broadest possible warrant, encompassing even first time visitors.

For all of these reasons, the district court's probable cause finding was not supported by the facts. Stripped of the false description of the website's appearance and taking the court's other probable cause findings at face value, all that remains is 1) Playpen was a Tor site; 2) visitors had to know the site's address; and 3) the FBI targeted everyone before they entered the site. These facts are insufficient to

support a finding of probable cause to believe that any and all visitors to Playpen were likely committing a crime.

### 2. The materiality of the application's false description of Playpen's appearance

As just shown, the false description of Playpen's homepage was so material that the lower court's probable cause determination cannot survive its excision. Were there any doubt about its materiality, this Court's en banc decision in *Gourde*, 440 F.3d 1065, lays them to rest. There, the Court found probable cause to search Gourde's computer based on his membership in a site that distributed child pornography. In reaching that determination, the Court focused on facts in the warrant application that showed Gourde was not merely an "accidental browser" or someone who, after taking a "free tour" of the site, "balked at taking the active steps necessary to become a member[.]" *Id.* at 1070; *see also id*. at 1071 ("The affidavit left little doubt that Gourde had paid to obtain unlimited access to images of child pornography knowingly and willingly, and not involuntar[il]y, unwittingly, or even passively").

The distinction between casual browsers or "balkers" and those who demonstrate intent to commit a crime is manifestly a critical one. Myriad websites offer legal sexual content, including child erotica, and the right to visit those sites is constitutionally protected. If a visitor could mistake Playpen for a legal "adult" site, fetish forum or chat room, there would be no probable cause to search a

visitor's computer merely because he or she was trying to access the site. *See generally American Civil Liberties Union v. Mukasey*, 534 F.3d 181, 187 (3d Cir. 2008) (finding Child Online Protection Act unconstitutional, noting that Internet material that is "harmful to minors" is still "constitutionally protected for adults.").

Accordingly, this Court carefully examined the warrant application in *Gourde* to determine whether it established Gourde was not just someone who unwittingly entered an illegal site or promptly "balked" when he found out what it contained. Significantly, the website in *Gourde* charged a membership fee and also allowed visitors to preview its contents *before* they joined the site. 440 F.3d at 1067. These facts demonstrated that Gourde intended to view and possess child pornography because, after having seen samples of what the site offered, he proceeded to purchase a membership, pay a recurring monthly fee, and maintain his membership over several months. *Id.* at 1070-71.

By contrast, the Virginia warrant application contained no particularized information about Mr. Tippens's interactions with the site or the activities of any other visitors. Moreover, the FBI offered free and immediate access to Playpen, without offering previews of its contents. Thus, the only indication first-time visitors would have had as to Playpen's purpose would have been the appearance of its homepage.

In *Gourde*, the warrant application established that the site at issue "unabashedly announced that its essential purpose was to trade child pornography."[20] First, the name of the site was "Lolitagurls.com" and the term "Lolita" is closely associated with a prurient focus on young girls. *Gourde*, 382 F.3d at 1014 (Gould, J. concurring in original panel decision). By contrast here, the name "Playpen" is not associated with child pornography, nor did the application claim that it was. Instead, the name is used by various mainstream "adult" enterprises, including a knock-off of "Playboy"; numerous strip clubs around the country; and legal websites (such as "Angel's Playpen" and "Xtreme Playpen") that feature explicit (but legal) pictures of young women. ER-S.VI 1089-95.

In addition, the Lolitagurls.com homepage in *Gourde* brazenly advertised its "Lolita pics," including "[o]ver one thousand pictures of girls age 12-17! Naked lolita girls with weekly updates!" 440 F.3d at 1067. By contrast, the FBI's homepage contained no references to child pornography, sexually explicit content, or anything else that "unabashedly announced" a criminal purpose. ER-S.VI 1083. At most, Playpen appeared to be some sort of erotic chat room or softcore site. *Compare* ER-S.VI 1083 *with* 1096 (results of Google search for "child models"); *see also United States v. Martin*, 426 F.3d 68, 75 (2d Cir. 2005) (probable cause

[20] This description of the website is from *United States v. Martin*, 426 F.3d 68, 75 (2d Cir. 2005), cited in *Gourde*, 440 F.3d at 1071, as involving "nearly identical facts[.]"

grounded on fact that, *inter alia*, "Candyman" site's "welcome message unabashedly announced" that it traded child pornography); *United States v. Shields*, 458 F.3d 269 (3rd Cir. 2006) (same).

Given these facts, or lack thereof, the Virginia application's claim that Playpen's homepage displayed pictures of "partially clothed prepubescent females with their legs spread apart" was critical. When the description of the site was false and the homepage actually displayed an unremarkable picture of a clothed young woman, the homepage could not function as a Fourth Amendment dividing line between casual browsers or "balkers" and those intending to view child pornography.

This is especially true because the Virginia warrant was anticipatory, with the "triggering event" for NIT searches being the act of logging in *while the site appeared as it had been described in the warrant application*. As this Court has explained, "[t]he execution of an anticipatory search warrant is conditioned upon the occurrence of a triggering event. If the triggering event does not occur, probable cause to search is lacking." *United States v. Vesikuru*, 314 F.3d 1116, 1119 (9th Cir. 2002).

Here, the NIT warrant authorized computer searches while visitors logged in to Playpen when it appeared *as described* in the warrant application, or at least displayed equally explicit images or otherwise announced its illicit purpose. Since

the actual appearance of the site was very different and much more benign than alleged, an essential triggering condition for the NIT searches was absent. Moreover, the Government made no effort to make Playpen's appearance conform to the description in its application or correct its misrepresentations and seek a new warrant. *See* ER-S.VI 1110-11. As this Court has held, if a warrant's "triggering events did not occur, the warrant was void, and evidence gathered from the search would have to be suppressed." *Vesikuru*, 314 F.3d at 1123.

For these reasons, and following *Gourde*, the false description of Playpen's homepage was material and this Court should suppress. *United States v. Perkins*, 850 F.3d. 1109, 1118 (9th Cir. 2017) (holding suppression appropriate when agents "provid[ed] an incomplete and misleading recitation of the facts" and did not provide copies of purportedly lascivious pictures, and thereby "effectively usurped the magistrate's duty to conduct an independent evaluation of probable cause").

### 3. The evidence unequivocally establishes that the false statements were made intentionally or recklessly

The Government's false statements in this case were particularly egregious because they were knowing and unjustifiable. The court below, having erroneously concluded that the false description of Playpen was "immaterial," made no findings about whether that falsehood was intentional or reckless. *See* ER.I 46. However, the undisputed facts show, at a minimum, recklessness.

Specifically, Lead Case Agent Daniel Alfin testified on cross-examination below that Playpen's homepage had displayed explicit pictures some time before the FBI took control of the site, but those images had been removed by the original administrator before the Government seized the site and applied for the Virginia warrant. Alfin also admitted that he saw the sanitized version of the homepage when he helped take control of Playpen the day before the warrant application was finalized, and he also helped prepare that application. ER-S.VI 1083, 1100-11. Yet, despite this knowledge (and his purported experience and expertise with child pornography investigations), Alfin did not correct the application.

Making matters worse, Alfin and other agents actively administered the site after it was moved to a government server (even posting announcements and updates for members). Once the FBI became the exclusive owner and operator of Playpen, all of the agents and technicians who maintained and constantly monitored the site would inevitably have seen its homepage. *See, e.g.*, ER-S.V 861. Given these facts, the false statements in the Virginia application were, at a minimum, reckless.

In sum, the warrant application contains no particularized information about Playpen visitors, even though the Government had such information about thousands of potential targets. Instead, it sought to target anyone who landed on the homepage, by falsely claiming that Playpen advertised itself as a child

pornography site and displayed sexual pictures of minors on its homepage. That falsehood was material and, at a minimum, reckless. The Court should therefore excise the false statements from the warrant application; find that there was no probable cause to search 100,000 or more computers without those statements; and order suppression of all fruits of the NIT search in this case.

### E. THE WASHINGTON WARRANT WAS ALSO BASED ON MATERIAL FALSE STATEMENTS, WITHOUT WHICH THERE WAS NO PROBABLE CAUSE TO SEARCH MR. TIPPENS'S HOME

One year after seizing Mr. Tippens's IP address and other data from his computer in Hawaii, the FBI and local police applied for a warrant to search his new home in Washington. In order to bridge that prolonged delay and establish a nexus between Hawaii and Washington, the application in support of the Washington warrant relied on two material allegations, both false.

First, the application falsely alleged that the Playpen pictures "candygirl123" had viewed in Hawaii were likely to be found in long term storage on his computer. Second, the application misleadingly alleged that the target of the search fit a "collector profile" and that "collectors" keep contraband "for many years." Because the record establishes that those falsehoods were at least reckless, this Court should order suppression of all evidence seized pursuant to the Washington warrant. *See generally Franks* 438 U.S. 154; *Condo*, 782 F.2d at 1506 (reviewing

court should excise false statements, include material omissions, and make *de novo* probable cause determination).

The court below appears to have concluded that the application's statements about the likelihood of finding evidentiary data were misleading, but not material, intentional or reckless. *See* ER.I 26-27, 29. The court also found that the application "lays a sufficient foundation for the collector profile to be applied to the user." ER.I 28. Both conclusions are erroneous and this Court should reverse.

### 1. The long term data storage claims in the Washington warrant application were both false and material

Because Playpen was on the Tor network, it was not true that pictures "candygirl123" had viewed in Hawaii and related data were likely to be found on Mr. Tippens's computer a year later. As a general matter, "[t]he critical element in a reasonable search is not that the owner of the property is suspected of a crime but that there is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought." *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978) (quotation marks omitted). Put another way, without a clear nexus between the location to be searched and the property that is sought, the warrant is invalid. *See, e.g.*, *United States v. Grant*, 682 F.3d 827 (9th Cir. 2012) (reversing denial of suppression motion because, despite clear evidence of criminality, there was insufficient nexus between the target residence and the evidence sought).

Further, even when there is probable cause to believe that the items would have been found at the specified location at *some* time, there must be probable cause to believe they will be found there *at the time of the search*. *Id.* at 835. Otherwise, the information will be deemed stale and the warrant is invalid.

In this case, the key question for determining probable cause is whether the Washington application established a sufficient nexus between the "candygirl123" Playpen visits in Hawaii and the Washington search a year later. This Court has treated digital evidence as having a longer shelf life than most physical evidence for probable cause purposes if there is also reason to conclude that the digital evidence can be found at a particular location. *See, e.g.*, *United States v. Hay*, 231 F.3d 630, 636 (9th Cir. 2000). Those cases are not relevant here, however, because the affidavit made false representations about whether Playpen files had been saved on the target computer in the first place. Moreover, Shook conceded during cross-examination below that his affidavit contains no facts indicating that Mr. Tippens moved a computer from Hawaii or had one at his Washington home. ER.II 199-200.

The application did state that "candygirl123" had been logged in to Playpen for a total of 26 hours and accessed pictures on two specific dates, but it did not allege that the user had actively copied or saved pornography, actions that would have been known to the Government through its control of Playpen's server and

the user data stored on it. *See* ER-S.V 939-941, 1032-33. Instead, the application described occasions when the visitor looked at pictures on the site and then indicates that those pictures were stored on the visitor's computer, in its "internet cache" or elsewhere, as an automatic function of viewing them. *See* ER-S.V 1037 at ¶ 34, 1042 at ¶ 51.

Had Playpen been on the regular Internet, the Government's assertions would have been plausible. The underlying premise of these allegations was that "[a]s the [defendant] viewed the images online and enlarged them on his screen, his computer automatically saved copies of the images to his 'internet cache.'" *United States v. Romm*, 455 F.3d 990, 993 (9th Cir. 2006); *see also id.* at 998 (holding that a defendant possesses child pornography when he knows that images will be automatically saved on his computer and has "the ability to copy, print, or email the images to others."). When a computer automatically saves copies of illegal pictures, a judge can conclude that illicit pictures were not just temporarily downloaded while viewed, but were likely stored on a long term basis on the computer.

But Playpen was a Tor site and Tor is specifically designed so users do not leave a data trail on their computers. This "disc avoidance" security feature prevents the type of automatic or "cache" storage that investigators rely on in typical Internet cases. *See* ER.II 168-177, 274-276; ER-S.V 761-764. Moreover,

while the Tor browser may not always block all "trace evidence" or "artifacts" (like the address of a site that the user visited), that type of data is typically stored in a computer's short term "volatile" or "random access memory." In this regard, both the defense and Government experts who submitted declarations below agreed (contrary to the trial court's conclusion) that "trace evidence" is routinely overwritten or deleted, and it is erased entirely each time a computer is turned off. ER.II 246-251, 264-265, 279-281; *see also* ER-S.V 1042-43 (Shook affidavit) at ¶ 51 (trace evidence and history files only remain "until overwritten").

None of the material facts about Tor were disclosed in the warrant application. ER.II 175 (where Shook admitted his omissions). If they had been, they would have established the *unlikelihood* of finding even "trace evidence" in Washington a year (or even a week) after the Internet activity that prompted the 2016 search. *See Liston v. Cnty. of Riverside*, 120 F.3d 965, 974 (9th Cir. 1997), *impliedly overruled on other grounds*, *Saucier v. Katz*, 533 U.S. 194 (2001) (false or missing information is material even if it would only have led magistrate to "require[] further information" before deciding probable cause). Plainly, if the warrant application had disclosed that it was unlikely that agents could recover forensic evidence from the target computer, there would have been no basis for authorizing a search. For these reasons, this Court should find that the court below erred in concluding that all of the false and omitted information was immaterial,

and that it clearly erred in finding Playpen pictures or related data "were almost certainly retrievable" a year after they were viewed. ER.I 33.

### 2. At a minimum, the affiant's false statements and omission of material facts was reckless

The record also establishes that the affiant was, at a minimum, reckless when he included false and misleading facts in the Washington application about long term data storage, and equally reckless when he omitted the facts about disc avoidance. Omissions can be just as reckless as misrepresentations. As this Court recently held in *Perkins*, suppression is required when agents provide "an incomplete recitation of the facts" and usurp the magistrate's duty to independently evaluate probable cause. 850 F.3d. at 1118. This is because "[t]he use of deliberately falsified information is not the only way by which police officers can mislead a magistrate when making a probable cause determination." *Stanert*, 762 F.2d at 781. "By reporting less than the total story, an affiant can manipulate the inferences a magistrate will draw," and "[t]o allow a magistrate to be misled in such a manner could denude the probable cause requirement of all real meaning." *Id*; *see also, e.g., Wilson v. Russo*, 212 F.3d 781, 787-88 (3rd Cir. 2000) (omissions are made with reckless disregard for the truth if an officer withholds facts when "[a]ny reasonable person would have known that this was the kind of thing the judge would wish to know"; failure to disclose difference in height between defendant and description of the assailant).

In this case, Det. Shook admitted below that he knew about Tor's security features and disc avoidance before he applied for the Washington warrant. ER.II 168. He also admitted he had consulted with others "experts" about Tor and related technical issues, and Lead Agent Daniel Alfin reviewed Shook's affidavit prior to its submission. ER.II 149; 191-92; *see also United States v. DeLeon*, 979 F.2d 761, 764 (9th Cir. 1992) ("[M]isstatements or omissions of government officials which are incorporated in an affidavit for a search warrant are grounds for a *Franks* hearing, even if the official at fault is not the affiant."). Tor's disc avoidance features are also explained on Tor's web site. And if all this were not enough to establish knowledge or at least recklessness, not only is the Tor network largely financed by the Government, but the FBI had designed sophisticated malware to penetrate Tor's defenses. All these facts render futile any claim that the misrepresentations and omissions in the Washington application were merely a mistake or oversight.

Nevertheless, the court below excused all of this by finding that Shook had a "theory" that "based on the viewing activity of user candygirl123, who found Website A, created a login account on the site, and then spent 26 hours on the site over a three-month period," there would at least be trace evidence of those activities on the target computer. ER.I 27. The court conceded that "[t]he theory is not airtight," *id.*, and in fact it is contradicted by the expert declarations submitted

below. At best, Shook's theory was speculative. *See generally United States v. Howard*, 828 F.2d 552, 555 (9th Cir. 1987) ("Mere speculation that a drug laboratory might exist in a home is not enough to establish the probable cause necessary to seize that residence.").

Moreover, even if the merits of Shook's "theory" are debatable, the dispositive fact is that he omitted all of the information that is inconsistent with that theory and misrepresented how Tor works in order to bolster it.

The trial court's ruling is all the more misguided because it concluded that Shook's "theory is strengthened in light of the collector profile," which was itself foundationless and misleading. *See* ER.I 27.

### 3. The boilerplate "collector profile" in the warrant application was foundationless and should be excised

The collector profile used in the Washington warrant application was without foundation because it was not tailored to Tor users such as Mr. Tippens. Collector profiles comprised of "boilerplate recitations designed to meet all law enforcement needs" are given little or no weight for probable cause purposes. *United States v. Weber*, 923 F.2d 1338, 1345 (9th Cir. 1990). In order to rely on such profiles, "the affidavit must lay a foundation which shows that the person subject to the search is a member of the class" of persons profiled. *Id*. When no such foundation was established in this case, the collector profile should not have been part of the lower court's probable cause determination. And, as already noted,

a reviewing court should excise false statements, include material omissions, and make a *de novo* probable cause determination. *Condo*, 782 F.2d at 1506.

The court below again conflated the characteristics of the regular Internet and Tor when it found computer users "including Tor users, in a strict sense [are] downloader[s] [who] also possess[] and receive[], which satisfied the foundation for the collector profile." ER.I 28-29. For the reasons explained below, this finding was clearly erroneous. Once the court found reliance on the boilerplate profile acceptable, it erroneously held that the profile "strengthened" Det. Shook's "theory" that trace evidence of child pornography would be found on Mr. Tippens's computer. ER.I 27. This Court should reverse the district court's holding.

Specifically, the warrant application's profile was not only (by the affiant's own admission) boilerplate, but it was also inapplicable to Tor users in critical respects. It claimed "collectors" such as Mr. Tippens keep contraband "*for many years*"; "typically" retain pictures and other media "*for many years*"; and "often" maintain digital collections in a secure environment, "usually" at the collector's residence. ER-S.V 1039 at ¶ 43(c) (emphasis added). The affidavit also asserted evidence that had been stored in Hawaii was likely to be found a year later and far away, since "collectors" keep images close by and for a long time in various ways *See* ER-S.V 1039-40 at ¶¶ 43-44.

But these claims describe a class of people diametrically opposed to Tor users. A primary benefit of the Tor network for people who view content on illicit sites is that they can do so without leaving a data trail or collecting images on their computers. ER.II 168-77; 274-76; ER-S.V 761-64. By employing security features that actively block storage of images and related data, Tor users act in a way that is inconsistent with an intent to collect pornography. They also act in a way that makes it less likely that they retain contraband for long period of times. Thus, the boilerplate profile did not apply to people like Mr. Tippens.

It is informative to contrast the instant boilerplate profile, where collectors were alleged to retain pictures and other media "for many years," "usually" at the collector's residence, with language used by the Government in earlier Virginia pleadings when it expressly discussed Tor users. ER-S.V 815-42 (applications for delayed notice of NIT searches). There the Government alleged that Tor users typically hasten to delete and destroy evidence because they are technically sophisticated and attuned to security issues and detection. Not only are Tor users highly concerned about security, the Government also alleged they are attentive to news about Internet investigations, share that information, and are likely to destroy evidence once an investigation becomes public. ER-S.V 819, 826, 833. News reports about Operation Pacifier and the FBI's use of NITs on the Tor network began circulating months before the Washington search, and it made national

headlines one month before. *See, e.g.*, Brad Heath, FBI Ran Website Sharing Thousands of Child Porn Images, USA Today (January 21, 2016).[21] The Government's characterization of Tor users therefore indicates that someone like Mr. Tippens would, in fact, have been *unlikely* to retain incriminating data on his computer by the time of the search.

Finally, not only was there no particularized showing that Mr. Tippens fit the collector profile, but Det. Shook testified that, at the time he prepared the application, it was equally likely that either Mr. Tippens or his mother was the person who had visited Playpen and was a "collector." ER.II 213-14 *see also* ER.S.V 1040 at ¶ 44. Shook also knew Mrs. Tippens was not living at the Washington house, a fact disclosed in the affidavit. Nevertheless, Shook included the profile and applied it just to Mr. Tippens because it was "standardized." ER.II 215-18.

For all these reasons, the district court clearly erred in finding Tor users are similar to the collectors described in the boilerplate profile used in the warrant application. Rather, use of the profile was without foundation under *Weber* and affirmatively misleading, and the profile could not be used to support probable cause to search Mr. Tippens's computer. When this Court excises from the warrant

[21] Available at: https://www.usatoday.com/story/news/2016/01/21/fbi-ran-website-sharing-thousands-child-porn-images/79108346/

application the foundationless profile as well as the affidavit's false claims that relevant images and data was likely stored on the target computer, and includes the true facts about Tor's security features, then only stale information about Playpen visits a year before the search will remain, with no nexus or fresh information connecting the Washington residence to that activity. Under these circumstances, this Court should suppress the fruits of the Washington search.

### F. THE GOVERNMENT CANNOT AVOID THE CONSEQUENCES OF ITS VIOLATIONS OF LAW AND THE FOURTH AMENDMENT BY INVOKING "GOOD FAITH"

The good faith exception to the exclusionary does not spare the Government from the consequences of its misconduct or the jurisdictional and Fourth Amendment violations in this case. This is true because 1) the Government searched property outside the explicit scope of the Virginia warrant; 2) its violation of Rule 41 was knowing and sanctioned by prosecutors and senior agents; 3) the Virginia warrant was based on intentionally false or reckless statements; and 4) the Washington warrant was also based on intentional or reckless false statements. *See generally United States v. Leon*, 468 U.S. 897, 919 (1984). The exclusionary rule is meant to deter just such "deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Herring v. United States*, 555 U.S. 135, 144 (2009). For these reasons, this Court should reject any invocation of good faith.

### 1. The Government cannot claim good faith when its search exceeded the geographic scope of the warrant

The Government cannot claim good faith when it searches and seizes property located in a place different from the location authorized by a warrant. *Gantt*, 194 F.3d at 1005 ("the good-faith exception is not relevant where the violation lies in the execution of the warrant, not the validity of the warrant"); *see* § B above. "[E]rrors in the execution of warrants are solely in the province of law enforcement agents [and] the good-faith exception has no applicability." *Id.* Here, consistent with her limited jurisdiction and authority, the Virginia judge signed a warrant that limited the NIT searches to computers in her district. The Government therefore cannot claim good faith when it searched a computer in Hawaii pursuant to that warrant.

### 2. The Government did not act in good faith when it deliberately violated Rule 41

The Government's deliberate violation of Rule 41 is also not subject to the good faith exception. *See* § C above. Whether violations of Rule 41 that are prejudicial or of constitutional magnitude can be excused under good faith is not entirely clear. In *Weiland*, this Court simply stated that suppression is "required" under such circumstances without reference to good faith. 420 F.3d at 1071 (quoting *Martinez-Garcia*, 397 F.3d at 1213). Moreover, the Court has expressly declined to apply the good faith exception to deliberate violations of Rule 41 even

when, as the court below erroneously concluded, the violation is "technical." *Gantt*, 194 F.3d at 1005 (suppressing when officers deliberately failed to serve complete copy of warrant on defendant, and concluding they acted deliberately when "the government has provided no explanation or justification for the agents' failure"). And, as explained above, the Government knowingly violated Rule 41 in this case.

Nevertheless, the court below concluded that the good faith exception applied to the Rule 41 violations because it found reliance on the warrant "objectively reasonable." ER.I 52. This conclusion ignores several facts and issues fatal to a claim of good faith. At a most basic level, the conclusion presumes the warrant was global and agents were entitled to rely on a global warrant. *See id*. However, the good faith exception does not apply when law enforcement agents rely on a facially overbroad warrant that effectively authorizes a general search. *United States v. Spilotro*, 800 F.2d 959, 968 (9th Cir. 1986) (rejecting claim of "good faith" and affirming suppression where warrant was so broad that officer could not reasonably rely on it). Hence, if the Magistrate Judge had authorized a global warrant, it was plainly overbroad and the Government cannot claim good faith.

The District Court's conclusion also ignored the undisputed facts establishing the Government's deliberate violation of the Rule. If the Rule itself

were not clear enough, DOJ's own computer search and seizure guidelines explained that the Rule did not allow for multi-jurisdictional computer searches. *See* § C(2)(b) above. Moreover, DOJ was particularly concerned about the ruling in *In re Warrant*, which denied an NIT warrant because it would have violated Rule 41, and the Government acknowledged the Rule's restrictions when seeking amendments to it. ER-S.V 866-70; s*ee also* ER-S.V 901 (Congressional Research Report on proposed Rule 41 amendments describing *In re Warrant* as "[p]erhaps the most prominent case" addressing the illegality of multi-jurisdictional NIT warrants).

The Government also cannot suggest that its violations were merely an error on the part of agents unfamiliar with what the law requires. Both the Virginia warrant application and all aspects of Operation Pacifier were reviewed and approved by prosecutors and senior agents. *See* ER.III 515-17; ER-S.V 946. As one court has observed, "it is one thing to admit evidence innocently obtained by officers who rely on warrants later found invalid due to a magistrate's error. It is an entirely different matter when the officers are themselves ultimately responsible for the defects in the warrant." *United States v. Reilly*, 76 F.3d 1271, 1281 (2d Cir. 1996), *on rehearing*, 91 F.3d 331. Indeed, the Supreme Court has held that responsible law-enforcement officers are expected to know "what is required of them" under the law and to conform their conduct to those rules. *Davis v. United*

*States*, 564 U.S. 229, 241 (2012) (concluding suppression not appropriate where officers acted in reliance on then-existing binding appellate precedent).

Contravening these basic tenets, two Courts of Appeal have excused the Government's violation of Rule 41 during Operation Pacifier pursuant to good faith. *United States v. Workman*, 863 F.3d 1313, 1315 (10th Cir. 2017) (assuming, "for the sake of argument," the Government violated Rule 41); *United States v. Horton*, 863 F.3d 1041, 1048 (8th Cir. 2017) (concluding the Government violated the Rule). Inexplicably overlooking *Davis*, both courts held that FBI agents could not be expected to know the requirements of Rule 41. *Workman*, 863 F.3d at 1320; *Horton*, 863 F.3d at 1052. Equally inexplicably, the courts overlooked the facts elucidated here regarding the Government's full knowledge of Rule 41's limits. And it was not just FBI agents who ignored the law, but also the prosecutor who approved the Virginia application and the senior DOJ and FBI personnel who were supervising as well. *See* ER.III 515-17; ER-S.V 946. For these reasons, the decisions in *Workman* and *Horton* are unpersuasive and this Court should reject any appeal to good faith in this case.

**3. The Government did not act in good faith when it made material false statements in the Virginia warrant application**

The Virginia warrant application's showing of probable cause turns on its false statements about Playpen's homepage and its purported advertising of child

pornography. *See* § D above. When the record establishes the Government was aware its description of Playpen was false before it sought the NIT warrant, the good faith exception does not apply. Good faith is not applicable if a warrant is based on intentionally or recklessly false material statements or omissions. *See, e.g.*, *Mills v. Graves*, 930 F.2d 729, 733 (9th Cir. 1991).

Not only did the Government provide false information to the Virginia judge in its warrant application, it also made no effort during the 15 days it operated the site to correct the application, even though the FBI had exclusive control of the site, was maintaining its homepage and searching computers that entire time. The Government demonstrated flagrant and prolonged disregard for meaningful judicial oversight of its unprecedentedly sweeping NIT searches, a disregard that cannot be reconciled with good faith.

#### 4. The Washington warrant was also based on material misrepresentations and omissions

This Court should hold the court below clearly erred in finding Det. Shook's false statements and boilerplate profile in the Washington application not intentionally misleading, false or reckless. *See* ER.I 26. Instead, the facts reveal his statements were, at a minimum, reckless. In this case, before he prepared the affidavit, Shook was aware of Tor's "disc avoidance" features making it unlikely illicit images and related data would be stored on the "candygirl123" computer and retrievable a year later. *See, e.g.*, ER.II 168. Nevertheless, Shook promoted the

opposite in the affidavit, maintaining that Playpen images and related data were likely to be found on Mr. Tippens's Washington computer, and omitted facts detailing Tor's security features.

Given Shook's admitted personal knowledge of the material omissions and misrepresentations, the trial court's finding that he consulted with other agents and also "relied on information from others including technical representations" only makes matters worse. ER.I 26; *see also DeLeon*, 979 F.2d at 764 ("[M]isstatements or omissions of government officials which are incorporated in an affidavit for a search warrant are grounds for a *Franks* hearing, even if the official at fault is not the affiant."). In addition, Shook employed a boilerplate collector profile that he knew was likely not applicable to Tor users. *See* § E(3) above.

The stark contrast between what Shook knew and what he told the magistrate judge is evidence of, at the least, a reckless disregard for the truth. The Government therefore cannot rely on the good faith exception in connection with the Washington search.

## IX. CONCLUSION

This Court should reverse Mr. Tippens's conviction and order the charge against him dismissed due to outrageous government conduct. If it does not order dismissal, the Court should order suppression of all fruits of the Virginia NIT warrant that relate to Mr. Tippens because that search exceeded the scope of the

warrant or, alternatively, because the warrant was issued and executed in violation of Rule 41.

The Court should also order suppression on the independent grounds that the Virginia warrant was not supported by probable cause and was based on material reckless or intentional falsities and omissions. Finally, the Court should order suppression on the independent grounds that the Washington warrant was based on material reckless or intentional falsities and omissions.

DATED this 13th day of October, 2017.

s/ *Colin Fieman*
Assistant Federal Public Defender
Attorney for David Tippens

## STATEMENT OF RELATED CASES

Counsel is not aware of any related cases now pending before this Court.

DATED this 13th day of October, 2017.

s/ *Colin Fieman*
Assistant Federal Public Defender
Attorney for David Tippens

## CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7)(B)(I), the attached brief is proportionately spaced, has a typeface of 14 points, and contains 19,527 words.

DATED this 13th day of October, 2017.

s/ *Colin Fieman*
Assistant Federal Public Defender
Attorney for David Tippens

## CERTIFICATE OF SERVICE

I certify that I filed the foregoing Opening Brief with the Clerk of the Court for the Ninth Circuit Court of Appeals by using the appellate CM/ECF system. I further certify that all non-sealed Excerpts of Record were electronically filed on this date. Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

I mailed one copy of this Opening Brief, first-class postage prepaid, to Mr. Tippens at his residence.

DATED this 13th day of October, 2017.

s/ *Amy Strickling, Paralegal to*
Colin Fieman,
Assistant Federal Public Defender