

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA,)	No. CR16-5110RJB
)	
Plaintiff,)	DEFENDANT’S SECOND MOTION
)	TO SUPPRESS EVIDENCE
v.)	
)	<i>[Oral Argument Requested]</i>
)	
DAVID TIPPENS,)	NOTED: February 3, 2016
)	
Defendant.)	

David Tippens, by and through his attorney, Colin Fieman, moves to suppress all evidence obtained through execution of a warrant at his residence in University Place, Washington. The pretrial motion deadline in this case is January 26, 2017. Trial is scheduled for February 27, 2017.¹

I. INTRODUCTION

Mr. Tippens’ first motion to suppress focused on the global NIT warrant that was issued in the Eastern District of Virginia. This motion addresses the subsequent warrant that was issued a year later to search Mr. Tippens’ home in University Place

¹Although the defense served comprehensive discovery demands on the Government on February 12, 2015, much of the discovery relevant to this motion (including exhibits C, D and E) was disclosed by the prosecution only recently. The Government has offered no explanation for why this evidence was not disclosed prior to the earlier motion deadlines set by the Court.

1 and seize his computer. *See* dkt. 37-3 (February 9, 2016, local warrants); exh. B
2 (affidavit in support of 2016 warrants).

3 The 2016 warrant fails to establish probable cause to believe that evidence or
4 instrumentalities of a crime would be found at that location. The crux of the warrant
5 application is that a visitor known as “candygirl123” used a computer with an IP
6 address assigned to Mr. Tippens’ residence in Hawaii to view pictures on the Playpen
7 website in February, 2015.

8 However, in September 2015, the Chief Legal Counsel for the FBI’s Hawaii
9 field office determined that “any legal inferences we can make about SFC Tippens
10 viewing, downloading or manufacturing child pornography is extremely low and
11 tenuous at best.” Exh. D. Consistent with this conclusion, the FBI rejected the Army’s
12 offer to postpone Mr. Tippens’ transfer to Washington and seek a warrant to search his
13 property while it was still in the custody of the Army’s shippers.

14 Approximately five months later, the FBI reversed course and decided to seek a
15 warrant in Washington. No new information is included in the 2016 warrant
16 application; it makes no showing that Mr. Tippens had Internet service at the new
17 residence, let alone a computer; and it offers no particularized facts establishing
18 probable cause to believe that any evidence that may have been found one year earlier
19 and several thousand miles away in Honolulu was likely to be found in University
20 Place.

21 Moreover, the FBI intentionally or recklessly omitted information that was
22 material to the Magistrate Judge’s determination of probable cause. The defense
23 requests a *Franks* hearing on the following four grounds:

24 First, the affidavit alleges that the user “candygirl123,” who was linked to Mr.
25 Tippens’ IP address in Hawaii, viewed various graphic pictures on the Playpen web site
26 in February, 2015. However, it does not allege that the visitor took any steps to

1 download or copy pictures or videos. Instead, in order to establish probable cause to
2 believe that illicit pictures or other evidence of a pornography offense would be found
3 on the Hawaii computer, the application alleges that copies of the pictures would have
4 been automatically saved on that computer when “candygirl123” viewed them. *See* exh.
5 B at ¶¶ 33-34. That claim is demonstrably false.

6 On the regular Internet, copies of web pages that a visitor views are
7 automatically copied onto the computer that is connected to that web page. The
8 opposite is true for the Tor network. As an added privacy and security measure, the Tor
9 browser, unlike regular Internet browsers, is designed to prevent automatic
10 downloading of web pages and related data. Since the affidavit does not allege that
11 there is any evidence (based on Playpen’s server records or otherwise) that
12 “candygirl123” saved, posted or distributed any illicit pictures, the FBI affirmatively
13 misled the issuing judge about the downloading and the likelihood of finding evidence
14 at the search location.

15 The second *Franks* issue undermines the application’s attempt to bridge the gap
16 between the time and place where someone visited the Playpen site (Hawaii) and the
17 location of the search (University Place). In this regard, the affidavit relies on a
18 “collector profile” to show that people who view and possess child pornography are
19 likely to keep it for a long time. Exh. B at ¶¶ 43-44.

20 Apart from the fact that this profile is boilerplate, it is recklessly or intentionally
21 misleading. As the Government itself has explained elsewhere, Tor users are *not* typical
22 Internet users or “collectors.” Instead, the Government has characterized Tor users as
23 technically sophisticated, sensitive to security and detection, and attentive to news that
24 may circulate about Internet investigations. Moreover, as already noted, the Tor
25 browser blocks automatic downloads, making the usual assumptions about continuing
26

1 possession of illicit pictures and related data that might apply to the average Internet
2 user inapplicable to Tor users.

3 The third *Franks* issue arises from the Government's disclosure of portions of
4 the FBI's investigation file. These records show that in October, 2015, agents obtained
5 a copy of the inventory for the personal property that the Army shipped to Washington
6 for Mr. Tippens. Exh. E. The inventory was prepared by the Army's movers and
7 includes a list of electronic devices, but no computers or digital storage devices are
8 listed on it. The affidavit makes no mention of this fact, and it contains no other facts
9 that might establish the presence of a computer devices at the Washington premises.

10 Finally, the affiant deliberately or recklessly misled the issuing judge by failing
11 to disclose that the FBI had previously decided that there was insufficient evidence to
12 support a warrant. *See* exh. D. The FBI reached this conclusion in September, 2015,
13 approximately six months after it had collected all of the evidence that it would later
14 rely on for the local warrant. The FBI's assessment of the evidence collected by the
15 NIT was not disclosed to the Magistrate Judge and it is inconsistent with many of the
16 opinions, inferences and conclusions that were presented to her.

17 II. STATEMENT OF FACTS

18 A. The Hawaii Investigation

19 The Court is already familiar with the original NIT warrant issued in the Eastern
20 District of Virginia and the facts leading up to the seizure of the IP address connected to
21 Mr. Tippens' prior residence in Hawaii. *See* dkt. 26 (First Motion to Suppress) at 2-7.

22 Law enforcement agents had identified the physical location associated with this
23 IP address in March, 2015. Exh. B at ¶ 36. The FBI office in Honolulu opened an
24 investigation into Mr. Tippens in June, 2015, in conjunction with the Army's Criminal
25 Investigation Division (CID). Later the same month, investigators confirmed that Mr.
26 Tippens resided with another adult (his mother) and his two minor daughters.

1 Concerned about the presence of children at the Hawaii residence, CID immediately
2 began coordinating with the FBI to obtain a warrant and search the house, including use
3 of a “SWAT” team.

4 For reasons that are unclear, the FBI was slow to respond to CID’s requests for
5 information needed to complete a warrant application. Meanwhile, Mr. Tippens was
6 ordered transferred to Joint Base Lewis McChord (JBLM), and the Army packed and
7 shipped his personal property on or about August 31, 2015. On September 22, 2015,
8 shortly before Mr. Tippens was scheduled to leave Hawaii, a JAG Senior Trial Counsel
9 who was involved in the investigation emailed the FBI’s lead case agent in Honolulu
10 and others to inform them that the Army could delay his departure and that the Army’s
11 shippers still had custody of his property, which had arrived in Washington. Exh. C.

12 Later the same day, the FBI’s Chief Division Counsel in Honolulu responded by
13 acknowledging that “[i]n the past, we usually requested your office to stop someone
14 from transferring to the mainland or overseas, but on this occasion, we are seeking the
15 opposite.” Exh. D. The Chief Division Counsel is the FBI’s top legal adviser for each
16 field office and his or her responsibilities include “assess[ing] the legal implications of
17 tools, technologies and techniques used by the FBI.”² According to the Chief Division
18 Counsel in Hawaii, “Currently, any legal inferences we can make about SFC Tippens
19 viewing, downloading or manufacturing child pornography is extremely low and
20 tenuous at best.” *Id.* The FBI therefore decided to hand off the investigation to its
21 Seattle office “to continue the investigation into his alleged child pornography
22 activities.” *Id.*

23 On October 1, 2015, the FBI added a copy of the “Government Bill of Lading”
24 for Mr. Tippens’ property to his case file. *See* exh. E. The moving company hired by
25

26 ² *See* <https://www.fbijobs.gov/career-paths/lega>, which describes the Chief Division Counsel’s
duties and qualifications.

1 the Army prepared a detailed inventory. It lists such electronic items as a camera, a
2 printer and a television, but no computers. This fact was not disclosed in the local
3 warrant application.

4 **B. The Washington Search**

5 On February 11, 2016, FBI agents assisted by local law enforcement executed
6 the local search warrant at Mr. Tippens' new home in University Place and, among
7 other property, seized a laptop computer.

8 The affidavit in support of that warrant states that user "candygirl123" logged on
9 to the FBI's Playpen web site for 26 hours on and before February 28, 2015. Exh. B at
10 ¶ 29. The affidavit links that user to Mr. Tippens' residence in Hawaii through an IP
11 address that had been seized by the FBI's NIT malware and describes various "posts"
12 that the user looked at while on the site. *Id.* at ¶¶ 27-36. The affidavit does not allege
13 that the visitor took any of the additional steps needed to intentionally download and
14 save posts, such as clicking on the "save as" option. The affidavit also does not claim
15 that the user posted any pictures; communicated with anyone about sharing pictures; or
16 otherwise indicated that he or she possessed pornography.

17 Instead, the affidavit alleges that the user's computer automatically saved copies
18 of the posts he/she had viewed when, "after accessing the post, the user clicked directly
19 on the described image *which would have resulted in downloading* another copy of the
20 image to the user's computer." Exh. A at ¶ 34 (emphasis added).

21 That statement is false. In truth, the Tor browser is configured to block
22 computers from automatically downloading copies of web pages and pictures that a
23 user views while on the Tor network, along with related browsing data. As explained in
24 the accompanying declaration of Prof. Matthew Miller, the regular Internet and the Tor
25
26

1 network work differently when it comes to storing data about user activity and web site
2 visits. *See* exh. A (Prof. Miller’s declaration and curriculum vitae).³

3 With the regular Internet, and with common browsers like Internet Explorer,
4 copies of web pages are automatically saved by the computer in a section of its hard
5 drive and memory called the “cache.” *Id.* at ¶ 3. Cache files are often fragmentary and
6 temporary; many people are unaware that their computers automatically save some files
7 in the cache; and these files are not listed in saved file directories. It is also relatively
8 difficult to locate and retrieve cache files unless a user knows where to look for them.
9 *Id.* Nevertheless, copies of web pages that are stored in cache files may have
10 evidentiary value and their presence may help support a search warrant.

11 Computers automatically save “cache” files to improve the speed with which
12 users can browse the Internet and view sites that they revisit. *Id.* at ¶¶ 3(c) and 5. For
13 example, if a user visits the front page of *The New York Times* site in the morning, his
14 or her computer will automatically save all or part of that page in the cache, regardless
15 of whether the viewer wants to save it. If the user decides to check the news again later
16 in the day, the computer can then retrieve a copy of the *New York Times* directly from
17 its cache and update it without having to reload all of the page from the newspaper’s
18 server. This direct access to web pages that a user has previously visited increases the
19 speed with which those pages can be displayed again. Over time, cache files may be
20 automatically deleted or overwritten by the computer without its users necessarily
21 knowing that the files were ever on the computer. *Id.* at ¶ 3(d).

22 The Tor network and its users are different because they prioritize privacy and
23 security over speed. In order to prevent computers from automatically downloading and
24 saving data from Tor sites, the Tor browser is programmed to do the opposite of regular

25 ³ The testimony of Government expert Prof. Brian Levine referenced in Prof. Miller’s
26 declaration at ¶ 8 is from the transcript of Levine’s testimony on November 1, 2016, at
pages 65-71.

1 Internet browsers: it blocks computers from automatically storing copies of web pages
2 that a user has visited. *Id.* at ¶¶ 5-6.

3 Anyone familiar with Tor would know this, since it is part of Tor’s special
4 privacy and security features. It is also explained on the Tor project’s web site. *See* Exh.
5 A at ¶ 7; *see also* Dkt. 37-1 (NIT warrant application) at ¶ 7 (“Information documenting
6 what Tor is and how it works is provided on the publicly accessible Tor website at
7 www.torproject.org”).

8 Further, the original NIT warrant application refers to this Tor security feature,
9 where it notes that Playpen notified visitors that “[t]his website is not able to see your
10 IP and cannot collect *or send any other form of information to your computer except*
11 *what you expressly upload.*” Dkt. 37-1 (NIT warrant application) at ¶ 13 (emphasis
12 added). The affidavit for the local warrant includes a summary of the very same
13 notification, but it omits the information about information blocking. *Compare* exh. B,
14 ¶ 16 *with* Dkt. 37-1, ¶ 13.

15 Although the affiant in this case stated that he has specialized training and
16 experience in investigating Internet and computer offenses, and that he had consulted
17 with other agents and experts involved in the Playpen investigation, there is no mention
18 of these Tor security features in his affidavit. *See, e.g.,* exh. B at ¶¶ 3-6. To the
19 contrary, the affiant affirmatively claims that “candygirl123” would have downloaded
20 Playpen images when he or she simply viewed them, even though that would not have
21 occurred.

22 C. The “Collector Profile”

23 The affidavit also includes a generic “collector profile.” *Id.* at ¶¶ 43-44. It states,
24 *inter alia*, that individuals who “access with intent to view and possess, collect, receive,
25 or distribute” child pornography “may” collect sexual images and use them in a variety
26 of ways; “typically” retain pictures and other media “for many years”; “often” maintain

1 digital collections in a secure environment, “usually” at the collector’s residence; and
2 “may” correspond with others and “rarely” destroy their correspondence. *Id.*

3 The affidavit does not address at all the characteristics, habits, or preferences of
4 Tor users, even though the Government has elsewhere stated that Tor users are
5 technologically sophisticated and not like typical Internet users or “collectors.”

6 For example, in its motions for delayed notification of the NIT searches, the
7 Government stated that “[u]sers of illegal child pornography websites on the Tor
8 network are extremely sensitive to law enforcement infiltration.” Exh. F (Requests for
9 Extension of Delayed Notice filed April 3, 2015; June 30, 2015; and September 24,
10 2015, in the Eastern District of Virginia) at Bates 415, 422 and 430. The Government
11 has also stated that Tor users tend to publicize and share information about law
12 enforcement methods, investigations, and how to conceal or destroy digital evidence.
13 *Id.* This, according to the Government, may result in “flight from prosecution, the
14 destruction of or tampering with evidence and otherwise seriously jeopardize the
15 investigation.” *Id.* at 416, 423 and 431.

16 The court in the Eastern District of Virginia relied on these representations about
17 Tor users, and the time sensitive nature of seizing information from them, when it
18 issued its delayed notice orders. *See* exh. G (EDVA delayed notice orders). None of this
19 information, however, was included in the local affidavit’s “collector profile.”

20 II. ARGUMENT

21 A. This Court Should Grant a *Franks* Hearing Because the FBI 22 Intentionally or Recklessly Misrepresented and Omitted Key Facts.

23 1. The Applicable Law

24 In *Franks v. Delaware*, 438 U.S. 154, 156 (1978), the Supreme Court held that
25 where a defendant makes “a substantial preliminary showing that a false statement
26 knowingly and intentionally, or with reckless disregard for the truth, was included by

1 the affiant in the warrant affidavit,” and that statement is material to a finding of
2 probable cause, courts are required to hold a hearing at the defendant’s request. The
3 doctrine applies to omissions as well as false statements. *United States v. Stanert*, 762
4 F.2d 775, 780-81 (9th Cir.), *amended by* 769 F.2d 1410 (1985).

5 The danger in omissions from an affidavit for search warrant are set forth in
6 *Stanert*:

7 The use of deliberately falsified information is not the only way by which
8 police officers can mislead a magistrate when making a probable cause
9 determination. By reporting less than the total story, an affiant can
10 manipulate the inferences a magistrate will draw. To allow a magistrate to
11 be misled in such a manner could denude the probable cause requirement
12 of all real meaning.

13 762 F.2d at 781.

14 Given these dangers, a defendant need not demonstrate that a judge would have
15 affirmatively denied the warrant if the true or missing information had been included.
16 Instead, the false or missing information is material even if it would only have led the
17 magistrate to “require[] further information” before deciding whether to grant the
18 warrant. *Liston v. Cnty. of Riverside*, 120 F.3d 965, 974 (9th Cir. 1997), *impliedly*
19 *overruled on other grounds*, *Saucier v. Katz*, 533 U.S. 194 (2001).

20 Once a *Franks* violation is established, the remedy is to include the omitted
21 information and exclude the false statements from the affidavit. *United States v. Condo*,
22 782 F.2d 1502, 1506 (9th Cir. 1986). The district court must then review the
23 “reformed” affidavit and make a *de novo* determination of probable cause, without the
24 usual deference to the issuing magistrate. *United States v. Kelley*, 482 F.3d 1047, 1051
25 (9th Cir. 2007). In addition, the Supreme Court explicitly precluded application of the
26 “good faith” doctrine to *Franks* violations, for the obvious reason that one does not act
in good faith when one recklessly or intentionally excludes material facts from a
warrant application. *See United States v. Leon*, 468 U.S. 897, 923 (1984).

1 In this case, there are four reckless or deliberate falsehoods or omissions, each of
2 which standing alone make the reformed affidavit lacking in probable cause,
3 particularly when viewed in conjunction with the lapse of time and distance between
4 the target's alleged activity on Playpen and the search.

5 **2. The First *Franks* Violation: The False Statements**
6 **About Downloading and Receipt or Possession of**
7 **Pictures.**

8 The affidavit does not allege that “candygirl123” knowingly or intentionally
9 downloaded child pornography. To the contrary, it describes various times when the
10 visitor looked at pictures on the site, and then alleges that those pictures were
11 downloaded by the visitor's computer as an inevitable function of viewing them. Exh.
12 B, ¶¶ 33-34.

13 The Government's premise here, as it has been with many other warrant
14 applications, is that “[a]s the [defendant] viewed the images online and enlarged them
15 on his screen, his computer automatically saved copies of the images to his ‘internet
16 cache.’” *United States v. Romm*, 455 F.3d 990, 993 (9th Cir. 2006); *see also id.* at 998.
17 (holding that a defendant can be convicted of possessing or receiving child pornography
18 when, “at a minimum,” he knows that the images will be automatically saved on his
19 computer and also has “the ability to copy, print, or email the images to others”).

20 Hence, when a computer automatically saves copies of illegal pictures in its
21 “cache,” a judge can conclude two things in the typical Internet case. First, illicit
22 pictures are likely to be found on the target computer, even if there is no evidence that
23 its user intended to possess or receive any pictures. Second, the cache pictures may
24 survive over time in a format that allows the user to later retrieve those pictures and
25 print, email or otherwise handle them in ways consistent with actual possession.

26 With Tor, however, pictures are not automatically saved on a target computer,
and there are no cache copies that a user can later retrieve and use. Unlike regular

1 Internet browsers, the Tor browser is designed to block automatic downloads. *See* exh.
2 A (Miller Declaration) at ¶¶ 3-7.

3 Moreover, Tor is popular because of its added security features, and its blocking
4 functions are explained on the Tor project’s web site, facts that should be well known to
5 an agent who claims relevant expertise. *Id.* at ¶ 7; Dkt. 37-1 (NIT warrant application)
6 at ¶ 7 (noting that “[i]nformation documenting what Tor is and how it works is provided
7 on the publicly accessible Tor website at ww.torproject.org”). Further, the original NIT
8 warrant refers to this Tor security feature, where it notes that the Playpen home page
9 announces that “[t]his website is not able to see your IP and cannot collect *or send any*
10 *other form of information to your computer except what you expressly upload.*” Dkt.
11 37-1 (NIT warrant application) at ¶ 13 (emphasis added). As previously noted, the
12 affiant here summarized and quoted parts of the very same notification, but left out the
13 most relevant part. *Compare id. with* exh. B, ¶ 16.

14 Given the true facts about the computer activity that occurred when visitors were
15 connected to Playpen, there was no probable cause to believe that the pictures described
16 in the affidavit (or any related data) would have been found at Mr. Tippens’ home in
17 Hawaii, let alone at his home in Washington a year later. Moreover, the affidavit does
18 not allege that the target visited sites other than Playpen, or offered any other basis for
19 concluding that he or she was in possession of contraband. As a result, the affidavit
20 affirmatively misled the issuing judge by presenting key facts as if this were a regular
21 computer and Internet case, when in fact the Tor network functions very differently.

22 Finally, the affidavit’s failure to disclose these facts was, at a minimum,
23 reckless. First, the affiant claimed that he had relevant technical expertise. Exh. B at
24 ¶¶ 2-4. The application also includes an entire section on Tor without disclosing that it
25 is designed to block automatic downloads. *Id.* at ¶¶ 9-12. Further, as previously noted,
26 the original NIT warrant application references the Tor project web site, which explains

1 the blocking functions, and the home page that the FBI maintained for Playpen refers to
2 that safeguard. And, of course, Tor is largely financed by the Government (which
3 provides up to 90% of its annual funding) and the FBI has designed malware to
4 penetrate Tor's defenses, rendering futile any claim that the FBI was unaware of how
5 downloads on Tor can or cannot occur. The Government also cannot credibly maintain
6 that it was not obligated to present the issuing judge with this information. *See, e.g.,*
7 *United States v. Chesher*, 678 F.2d 1353, 1362 (9th Cir. 1982) (failure of officer having
8 extensive contacts with other investigators to discover that defendant was no longer
9 with Hell's Angels, contrary to assertion in affidavit, constituted sufficient showing of
10 intentional or reckless falsity to warrant *Franks* hearing; reversing denial of hearing);
11 *United States v. Comprehensive Drug Testing, Inc.* 621 F.3d 1162, 1178 (9th Cir. 2010)
12 (Kozinski, J., concurring) (CDT) ("a lack of candor in [any] aspect of the warrant
13 application must bear heavily against the government in the calculus of any subsequent
14 motion to return or suppress the seized data.").

15 In short, once the false information about saved files is excised from the
16 application and the true facts about Tor are added, there is no basis to conclude that
17 copies of contraband pictures would have been found in Hawaii, let alone a year later in
18 a different place. As a result, the issue in this case is not just whether the affidavit
19 establishes that evidence was still on the premises by the time the search occurred.
20 Rather, the affidavit misled the court about whether the evidence was ever present at all
21 in Hawaii, and even more so as to its possible presence in Washington.

22 3. The Second *Franks* Violation: The False and Misleading 23 "Collector Profile."

24 The affidavit also misled the court by including a false "collector profile." The
25 profile is material because without it there is no basis for concluding that evidence or
26

1 contraband related to the alleged criminal activity in Hawaii would likely be found a
2 year later in Washington. The profile was misleading in two critical respects.

3 First, the affidavit sought to connect the original Hawaii search location with the
4 Washington search location through the profile by falsely asserting that “Tippens or a
5 resident of the SUBJECT PREMISES displays characteristics” that fit the profile. Exh.
6 A at ¶ 44 (capitalization in original). Without the profile, and in particular its assertion
7 that such “collectors” keep contraband “for many years” (*id.* at ¶ 43(c)), the rest of the
8 information in the affidavit is both stale and fails to establish a nexus between the
9 alleged criminal activity and the location to be searched.

10 According to the Government itself, however, Tor users are not typical of child
11 pornography offenders. To the contrary, the Government has maintained that Tor users
12 are very different from the average Internet user and offender because they are
13 technically sophisticated and highly attuned to security issues and possible detection.
14 *See* exh. G; *see also, e.g., United States v. Michaud*, CR15-0531RJB. Dkt. 47 (Govt.
15 Response to Motion to Suppress) at 25 (describing how Playpen was “no ordinary, run-
16 of-the-mill website” and how its visitors are especially security minded and technically
17 sophisticated).

18 Equally importantly, the Government has stated that Tor users are attentive to
19 news about Internet investigations, share that information on Internet bulletin boards
20 and in other forums, and are likely to conceal or delete evidence once an investigation
21 becomes public. *Id.* In this case, news reports about Operation Pacifier began
22 circulating in October 2015, and there were also reports about the FBI’s use of NITs on
23 the Tor network much earlier, long before the Washington search. *See also, e.g., United*
24 *States v. Michaud*, dkt. 39 (Government’s November 6, 2015, Response to Motion to
25 Vacate or Modify Protective Order) at 4 (where it argued that, once the Playpen
26

1 investigation or the FBI's use of NITs became public, the targets may conceal or
2 destroy evidence and jeopardize ongoing investigations).

3 None of that information was included in the instant warrant application, for the
4 obvious reason that Tor users do not actually fit the profile that the Government
5 presented. It would also have caused the issuing judge to focus more on the delay in
6 seeking a warrant, which the profile was designed to minimize. Further, if the affidavit
7 had included the characteristics of Tor users that the Government has alleged
8 elsewhere, those characteristics would have weighed heavily against probable cause to
9 believe that evidence was likely to be found in Washington.

10 The profile is also false and misleading for a reason directly related to the
11 affidavit's misrepresentations about automatic downloading. *See* § II(A)(2), *supra*. Tor
12 users, by utilizing the network security features that block automatic downloading, act
13 in a way that is *inconsistent with* an intent to "possess, collect, receive, or distribute."
14 *See* exh. B at ¶ 43 (a)-(e) and (g). They also act in a way that makes it *less* likely that
15 they retain contraband, or any evidence that they viewed contraband, for any period of
16 time, let alone for a year or more. Obviously, if someone wants to collect and retain
17 child pornography on their computer, that person is unlikely to take affirmative steps to
18 avoid receiving copies of the pornography. Since the affidavit contains no particular
19 facts related to "Tippens or a resident" of the Hawaii house that might otherwise show a
20 propensity to collect and retain (such as purchasing pornography, intentional
21 downloading, or membership in non-Tor sites), the "collector profile" is not only
22 irrelevant to the facts in this case, but affirmatively misleading.

23 The inclusion of this profile is particularly egregious because the Ninth Circuit
24 long ago criticized "collector profiles" that consist of "boilerplate recitations designed
25 to meet all law enforcement needs." *United States v. Weber*, 923 F.2d 1338, 1345 (9th
26 Cir. 1990). In *Weber*, the Ninth Circuit held that "if the government presents expert

1 opinion about the behavior of a particular class of persons, for the opinion to have any
2 relevance, the affidavit must lay a foundation which shows that the person subject to the
3 search is a member of the class.” *Id.* at 1345.

4 In this case, the Government presented one description of Tor users to the court
5 in Virginia to support its applications for delayed notice authorizations, as well as
6 oppose motions to unseal and make various other arguments here. *See* exh. F. It
7 presented a different “profile” in the Washington affidavit that not only does not fit Tor
8 users, but omitted all the facts that were inconsistent with that profile. As a result, the
9 affidavit’s profile not only fails to lay a foundation that shows that it relates to the
10 relevant class; it also omitted all of the facts that were inconsistent with the conclusions
11 that the Government wanted the court to draw about the target’s habits and whether or
12 not the particularized information was stale.

13 Indeed, even if this case did not involve Tor users, the collector profile would be
14 essentially worthless. The malleability of the “expert” opinions that supposedly inform
15 these profiles is demonstrated by the Government’s recent reliance on an expert opinion
16 that reached different conclusions about the typical person who views child
17 pornography:

18 Many users elect to view the files they download, get their gratification and then
19 delete the files. Users who do this have either decided to do this out of fear of
20 being caught by their significant other or out of a simpl[e] though[t] process
21 [whereby] they [know] the files are out there and they can re-download them at
22 anytime they want to get their next gratification. Some users feel guilty about
their habits and discard all files and then when their need for gratification
surpasses their guilt they download again.

23 Exh. H at 5 (excerpts of Government expert report and accompanying CV in *United*
24 *States v. Hart*, CR14-5507RBL). The Government offered this expert opinion in a
25 recent case where it needed to account for the absence of pornography on a computer,
26 and it clearly would not serve the Government’s purposes in the instant warrant

1 application. Here, rather than showing why pornography might not be found on a
2 computer, the FBI had to persuade the court that it could still be found on a computer
3 long after the alleged viewing. As a result, these cases offer a perfect example of how
4 so-called profiles can be “designed to meet all law enforcement needs.” *Weber*, 923
5 F.2d at 1345.

6 In *Weber*, the court reversed the denial of a suppression motion, and rejected the
7 Government’s assertion of “good faith,” because the “foundationless” collector profile
8 was material to finding probable cause to believe that evidence would be found at the
9 defendant’s home just four months after he had placed an order for apparent child
10 pornography. *Id.* at 1346. Likewise, in this case the profile was material to determining
11 probable cause to believe that evidence would be found in Washington, since without it
12 there is no basis at all for concluding that it would be there, a year after the alleged
13 viewing and thousands of miles from the place where it allegedly occurred.

14 In short, the “collector profile” was boilerplate; devoid of facts linking the
15 profile to particular facts in the case; and inconsistent with expert opinions the
16 Government has relied on in other cases. Most importantly, the profile is not relevant to
17 Tor users, who the Government has elsewhere said have characteristics very different
18 from the typical “collector” that are inconsistent with collecting contraband or storing
19 inculpatory data on their computers for long periods of time. The Court should
20 therefore excise the profile from the affidavit, which leaves only stale and misleading
21 information about alleged downloading a year earlier at a different location.

22 **4. The Third *Franks* Violation: The Missing Facts About Mr.**
23 **Tippens’ Relocation to Washington.**

24 The affidavit was also intentionally or recklessly misleading because it did not
25 disclose that Mr. Tippens’ move from Hawaii to Washington was coordinated between
26 the FBI and the Army and that the inventory of his property did not include a computer.

1 The affidavit does not offer any basis for concluding that Mr. Tippens otherwise
2 transported a computer to Washington. While many people have laptop computers, the
3 affidavit does not suggest that “candygirl123” used a laptop or that Mr. Tippens owned
4 one. In fact, it offers nothing to indicate that he had *any* computer, or even Internet
5 access, at his new home.

6 Thus, even assuming that an excised and reformed affidavit establishes probable
7 cause to believe that Mr. Tippens (or another resident of his Hawaii home) had viewed
8 pornography in early 2015, there was no probable cause to believe that the target
9 computer or related evidence would be found in Washington in 2016.

10 “The critical element in a reasonable search is not that the owner of the property
11 is suspected of crime but that there is reasonable cause to believe that the specific things
12 to be searched for and seized are located on the property to which entry is sought.”

13 *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978) (quotation marks omitted). Put another
14 way, without a clear nexus between the location to be searched and the property that is
15 sought, the warrant is invalid. *See, e.g., United States v. Grant*, 682 F.3d 827 (9th Cir.
16 2012) (reversing denial of suppression motion because, despite clear evidence of
17 criminality, there was insufficient nexus between the residence and the evidence
18 sought); *United States v. Hove*, 848 F.2d 137, 139 (9th Cir. 1988) (same).

19 Further, even when there is probable cause to believe that the items would have
20 been found at the specified location at *some* time, there must be probable cause to
21 believe they will be found there *at the time of the search*. Otherwise, the information
22 will be deemed stale and the warrant is invalid. “While conclusive evidence of guilt is
23 of course not necessary under this standard to establish probable cause, “[m]ere
24 suspicion, common rumor, or even strong reason to suspect are not enough.” *Torres v.*
25 *City of Los Angeles*, 548 F.3d 1197, 1206-07 (9th Cir. 2008) (citations omitted).

1 Some courts have given digital evidence a longer shelf life for probable cause
2 purposes when there was also probable cause to conclude that the data would be found
3 at a particular location. *See, e.g., United States v. Hay*, 231 F.3d 630, 636 (9th Cir.
4 2000) (relying in part on affidavit’s assertion that even if files were on a computer, they
5 could be retrieved, even if deleted). Those cases are not relevant here, however, because
6 the affidavit made false representations about whether files had been downloaded from
7 Playpen in the first place. *See* § II(A)(2), *supra*. Hence, the affidavit not only recklessly
8 or deliberately omitted the fact that Mr. Tippens’ moving records show that he did not
9 ship a computer to Washington, it also misled the court about whether the evidence
10 detailed in the affidavit was likely present even before he was transferred.

11 Under these circumstances, there can be no credible dispute that the Magistrate
12 Judge should have been presented with all the facts material to determining whether
13 evidence of a crime allegedly committed in Hawaii was likely to be found much later in
14 Washington. Given the false information contained in the affidavit about whether
15 pictures had been downloaded from Playpen a year earlier; the lack of any information
16 about whether there was a computer or even Internet service at the search location; and
17 the absence of any other facts that might bridge the one-year gap between Hawaii and
18 Washington, the property inventory weighs significantly against a finding of probable
19 cause. And, since the FBI had received a copy of the inventory months before it applied
20 for the warrant, the only explanation for its failure to disclose the inventory is that it is
21 inconsistent with the conclusions that the FBI wanted the court to reach about the
22 probability of finding evidence in Washington.

23 **5. The Fourth *Franks* Violation: Omission of the FBI’s**
24 **Assessment of Whether it Would Actually Find Any Evidence**
25 **if Mr. Tippens’ Property was Searched.**
26

1 In the warrant application, the affiant states that he has probable cause to believe
2 that contraband and evidence would be found at Mr. Tippens' home based not only on
3 his own opinion and expertise, but the opinions and expertise of other agents who were
4 familiar with the case. Exh. B at ¶¶ 5 and 6. These statements are important because the
5 application involves novel and complex technical issues. Accordingly, the Magistrate
6 Judge necessarily relied in large part on the FBI's conclusions about the reliability of
7 the investigative techniques described in the application and the inferences that could
8 be drawn from the computer activities that it describes.

9 While asserting reliance on the conclusions of others, the affiant misled the
10 judge because he did not disclose that the FBI had previously concluded that there was
11 insufficient evidence to proceed with a more timely search of Mr. Tippens' property.
12 Specifically, the Chief Division Counsel in Hawaii memorialized the FBI's conclusions
13 in correspondence with the Army's CID in September, 2015. The Chief Division
14 Counsel serves as the top legal adviser for each FBI field office and, according to the
15 FBI's job descriptions, his or her responsibilities include assessing "the legal
16 implications" of any "technologies and techniques" used by the FBI, which presumably
17 includes the implications of the "Network Investigative Technique" evidence as well.
18 Consistent with that duty, Tony Lang, the Chief Division Counsel for the Honolulu
19 field office, wrote to the CID that "any legal inference we can make about SFC Tippens
20 viewing, downloading or manufacturing child pornography is extremely low and
21 tenuous at best." Exh. D. The FBI communicated this assessment to CID after the Army
22 had offered to postpone Mr. Tippens' transfer to Washington and search his property,
23 which the Army was still in the process of moving. Exh. C.

24 At the time, the FBI had all of the information that the affiant would later
25 summarize in the Washington warrant application. Specifically, the FBI had deployed
26 its NIT months earlier and already collected all of the information about "candygirl123"
that was included in that application.

Further, no new facts or information emerged after Mr. Tippens left Hawaii that
might have added to probable cause. To the contrary, the only facts that developed

1 between the time that Mr. Tippens left Hawaii and the application in Washington are
2 that he did in fact move; there was no evidence that he took a computer with him; and a
3 substantial amount of additional time had passed. Moreover, the Chief Division
4 Counsel was not just expressing his personal opinion about the available evidence, but
5 spoke of the conclusions that “we” (i.e. the FBI, or at least the field office as a whole)
6 had reached about the investigation.

7 The conclusions memorialized by the Chief Division Counsel are important
8 because they are inconsistent with conclusions and inferences that the affiant did
9 include in the Washington application, which is heavily reliant on expert opinions about
10 the reliability of the NIT evidence and the legal inferences that can be drawn from it. As
11 explained in *Stanert*, 762 F.2d at 781, “[b]y reporting less than the total story, an affiant
12 can manipulate the inferences a magistrate will draw. To allow a magistrate to be
13 misled in such a manner could denude the probable cause requirement of all real
14 meaning.” The omission of the Chief Division Counsel’s conclusions are particularly
15 material because, as noted, he is responsible for assessing the “legal implications” of
16 the FBI’s tools and techniques. It therefore appears that he, and others in the Hawaii
17 field office as well, were less than confident about the reliability of the NIT evidence or
18 the probability of finding evidence of a crime based on it, particularly since there were
19 no other evidence establishing possible possession of contraband.

20 Equally importantly, “an officer’s consultation with a government attorney is of
21 significant importance to a finding of good faith.” *United States v. Brown*, 951 F.2d
22 999, 1005 (9th Cir. 1991). Here, the Chief Division Counsel’s conclusions were part of
23 the FBI’s case file, and the affiant therefore knew or should have known that the
24 government attorney who had reviewed the evidence in the district where the alleged
25 crime had occurred had concluded that the evidence that Mr. Tippens had viewed child
26 pornography, let alone possessed it, was too tenuous to support a warrant. This fact
should have been disclosed to the Magistrate Judge because it was material to her
evaluation of the conclusions and inferences that the affiant did include. *Cf. United
States v. Ryan*, 153 F.3d 708, 712 (8th Cir. 1998) (reflecting that district court

1 concluded and Government conceded that undisclosed opinion of Government expert,
2 who disagreed with Government's other experts, was exculpatory under *Brady*, but
3 concluding that disclosure would not have changed outcome); *Paradis v. Arave*, 130
4 F.3d 385, 395 (9th Cir. 1997) (finding *Brady* violation in failure to disclose that
5 Government expert had previously had contrary opinion).

6 **B. The Affidavit Fails to Establish Probable Cause that Evidence**
7 **Would be Found at Mr. Tippens' Washington Residence.**

8 Even without all the false statements and omissions, the Court should find that,
9 given the totality of the circumstances, probable cause for a search of Mr. Tippens'
10 home went from "extremely low and tenuous at best," as the FBI had concluded in
11 September, 2015, to virtually nonexistent and entirely stale.

12 As a general matter, a warrant violates the Fourth Amendment if it is based on
13 facts that are too remote in time to establish probable cause to believe that evidence will
14 be found at the location to be searched. "[I]t is manifest that the proof must be of facts
15 so closely related to the time of the issue of the warrant as to justify a finding of
16 probable cause *at that time*." *Durham v. United States*, 403 F.2d 190, 193 (9th Cir.
17 1968) (*quoting Sgro v. United States*, 287 U.S. 206, 210 (1932)) (emphasis added).

18 Even "[t]he most convincing proof that the property was in the possession of the
19 person or upon the premises at some remote time in the past will not justify a present
20 invasion of privacy." *Durham*, 403 F.2d at 193. While the Ninth Circuit has upheld
21 warrants that are based on information that may be relatively remote in time, in each
22 case the affidavit demonstrated either a continuing pattern of suspicious activity or
23 recent facts that corroborated and refreshed earlier illegal activity. Thus, in *Grant*, the
24 Ninth Circuit held that "a 'mere lapse of substantial amounts of time,' does not
25 undermine a warrant *if 'a continuing pattern or other good reasons' suggest that the*
26 *evidence sought remains in the location to be searched[.]*" 682 F.3d at 835 (citation
omitted). "In other words, because evidence can be moved or disposed of, the affidavit

1 must support an inference that it is presently in the residence to be searched, regardless
2 of its past position.” *Id.* This is particularly true here, where the Government has
3 emphasized the time-sensitive nature of the Operation Pacifier searches because of the
4 possible disposal or destruction of evidence once the operation became known. *See* exh.
5 G.

6 Moreover, the lack of probable cause to search in Washington results not only
7 from the prolonged passage of time and the distance between where the alleged
8 connection to Playpen occurred and the search location. It also results from the fact that
9 the evidence that the affidavit relies on (pictures purportedly downloaded from
10 Playpen) was never in the “past position” either, since the affidavit misled the court
11 about alleged downloading in the first place. *See* Section II(A)(2), *supra*.

12 Further, the affidavit does not allege that there was any “continuing pattern” or
13 recent activity that might “freshen” the otherwise stale information. In fact, apart from
14 establishing that Mr. Tippens lived at the new Washington residence, the affidavit
15 contains no information whatsoever beyond what the FBI in Hawaii had concluded was
16 “extremely low and tenuous at best” a year earlier.

17 It is also apparent that the FBI did not believe that Mr. Tippens had a continuing
18 interest in child pornography, since it knew that he had custody of two minor children
19 and not only decided not to pursue a warrant in Hawaii, but waited many additional
20 months to apply for a warrant in Washington.⁴

21
22 ⁴ Given the FBI’s lack of urgency (in contrast to that of Army investigators, who were
23 pushing the FBI to obtain a timely warrant in Hawaii to help ensure the safety of Mr.
24 Tippens’ children), it is fortunate for the Bureau that Mr. Tippens is a loving and
25 responsible parent. In this regard, his relationship with his daughters (ages 16 and 18)
26 has been thoroughly investigated by Child Protective Services and law enforcement,
which have concluded that he has taken good care of them. In addition, a polygraph
examination has confirmed that Mr. Tippens has never had inappropriate contact with a
child, and there is no allegation that he ever did. Mr. Tippens’ children are now living
with an aunt in Texas.

1 Finally, as discussed above, the Government has historically relied on a
2 “collector profile” to try to compensate for otherwise stale information. The problem
3 here is that the affidavit’s collector profile is itself false and misleading. *See* section
4 II(A)(3), *supra*. Perhaps most problematically, the Government has repeatedly claimed
5 in other filings that Tor users are typically sensitive to detection and takes steps to avoid
6 it; monitor the news and share information about Internet and Tor investigations; and
7 may conceal, discard or destroy evidence once the Playpen investigation became public.
8 Obviously, those characteristics make it far less likely that any evidence would be
9 found by the time the FBI decided to search Mr. Tippens’ Washington home,
10 particularly since the FBI had shut Playpen down almost a year earlier and news of the
11 Playpen investigation had been circulating widely. Yet none of these facts were
12 included in the local warrant application.

13 With no other information linking the search location to the alleged crime, there
14 is no probable cause to support the Washington warrant.

15 **C. The “Good Faith” Exception Is Inapplicable.**

16 The Government cannot invoke the good faith exception to rescue the affidavit.
17 As noted earlier, the Government is foreclosed from relying on the exception when the
18 affidavit includes false or materially misleading information, or omits material
19 information. *Leon*, 468 U.S. at 923. The application is also patently defective given the
20 lapse of time, the new and unrelated location of the search, and the lack of any
21 evidence, apart from the boilerplate and false collector profile, that the target of the
22 search was in fact a collector. *See Weber*, 923 F.2d 1338, 1345 (reversing denial of
23 suppression motion, and finding no good faith, in part because “[i]t goes without saying
24 that the government could not search Weber’s house for evidence to prove Weber was a
25 collector merely by alleging he was a collector.”).

1 While warrant affidavits are not to be reviewed in a “hypertechnical” manner,
2 they still must be carefully analyzed to ensure that the proposed inferences of probable
3 cause to search in fact hold up. The Ninth Circuit decision in *Grant* is a good example
4 of that. The Ninth Circuit concluded, as had the district court, that the affidavit did not
5 establish probable cause that the items sought would be at the particular location. 682
6 F.3d at 832-35. The affidavit in *Grant*, thirteen pages with 50 exhibits,⁵ contained a
7 wealth of information purporting to link the premises to the cell phone that was sought.
8 For example, the affidavit alleged that one of the homeowner’s son’s was connected to
9 the gang suspected of being involved in the murder; had pawned the victim’s
10 Blackberry; had possessed the phone after the murder; and had possessed a gun looking
11 like the murder weapon. *Id.* at 829-31, 832-33. The affiant also tied another son of the
12 homeowner to the suspected gang, the description of the perpetrator, the city in which
13 the crime had occurred, and another individual in contact with the victim’s telephone
14 after the murder. *Id.* at 829-31, 833-35. The affiant then attempted to link both sons
15 with the homeowner and his residence. *Id.* at 829-31, 832-35.

16 The Ninth Circuit reviewed each thread of inference in detail to show that, when
17 analyzed carefully, in fact there was insufficient validity to the inferences that the
18 affiant wanted to draw. In *Grant*, there was no question that the affidavit established
19 criminality; the weak link was the nexus of the particular premises to the items the
20 warrant sought. *Id.* at 840.

21 The *Grant* court not only found a lack of probable cause, but also reversed the
22 district court’s ruling applying the good faith doctrine. *Id.* at 832-36. It did so despite
23 the significant amount of information in the affidavit, and two separate potential links
24 between the property and the gun that was sought. *Id.* at 832-35. The court concluded
25

26 ⁵ See *Government's Answering Brief*, No. 11-50036, 2011 WL 9680355, at *12 (9th Cir. Oct. 6, 2011).

1 that, despite all the information in the affidavit, ultimately there was no substance to the
2 inference that the gun would be found at that particular location. The same conclusion
3 applies to any inference that the instant affidavit established the presence of evidence at
4 Mr. Tippens' home. *See also CDT*, 621 F.3d at 1177 (admonishing trial courts to be
5 particularly attentive to inferences that the Government promotes in digital evidence
6 cases and to exercise "greater vigilance" when reviewing warrants involving computer
7 searches).

8 Finally, as previously noted, "an officer's consultation with a government
9 attorney is of significant importance to a finding of good faith." *Brown*, 951 F.2d at
10 1005. The affiant in this case inevitably knew that the Chief Division Counsel in
11 Hawaii had concluded that there were insufficient grounds to obtain a warrant to search
12 Mr. Tippens' property, since that conclusion was made part of the case file.

13 IV. CONCLUSION

14 This Court should either suppress the fruits of the warrant or first grant a *Franks*
15 hearing, after which it should suppress.

16 DATED this 26th day of January, 2017.

17 Respectfully submitted,

18 s/ Colin Fieman
19 Colin Fieman
20 Attorney for David Tippens
21
22
23
24
25
26

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

CERTIFICATE OF SERVICE

I hereby certify that on January 26, 2017, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to all parties registered with the CM/ECF system.

s/ Amy Strickling, Paralegal
Federal Public Defender Office