JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. DAVID TIPPENS, Defendant.	No. CR16-5110RJB DEFENDANT'S REPLY TO GOVERNMENT RESPONSE TO SECOND MOTION TO SUPPRESS EVIDENCE *[Oral Argument Requested]*

I. REPLY ARGUMENT

The Government devotes most of its response to knocking down a straw man. After reviewing all of the facts about Playpen's appearance and content, the Government concludes, "Indisputably, Playpen and its members had one goal in mind: to further the sexual exploitation of children through the creation and distribution of child pornography." Govt. Response at 8.

Setting aside the fact that there is no claim in the warrant application that "candygirl123" created or distributed anything (it was the FBI that was doing most of the distributing), the Supreme Court long ago held that "[t]he critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that the specific things to be searched for and seized

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

are located on the property to which entry is sought." *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978).

Given this law, the issue here is not whether there was reason to believe that "candygirl123" had viewed child pornography in Hawaii a year before the search of Mr. Tippens' home in Washington. Instead, "the critical element" is whether there was probable cause to believe that evidence of a crime would be found there. With the issue properly framed, a review of the undisputed facts shows that the application at least recklessly misrepresented and omitted a host of material facts.

A. The Government's Expert Declaration Confirms that the Warrant Application Falsely Claimed that Child Pornography Was Stored on the Target Computer.

In his declaration, FBI Forensic Examiner John Powers agrees with defense expert Prof. Matthew Miller on all the material facts. Powers acknowledges that the Tor browser "is designed with security and privacy features intended to reduce the traceability of a user's web activity," and he does not dispute that these features block downloading from sites like Playpen. Govt. Response to Second Motion to Suppress, exh. A (Powers Declaration) at ¶ 4.

Powers goes on to state that Playpen content was "viewable and therefore downloaded at least *while the user is viewing it*." *Id*. at ¶ 7 (emphasis added). Mere viewing is not downloading, since the common definition of downloading is "an act or instance of transferring something (as data or files) from a usually large computer to the memory of another device ([such] as a smaller computer)."[1] But even accepting Powers' broad use of the term "download" as including viewing, rather than saving something in a computer's long term memory, his statement is both true and irrelevant.

[1] https://www.merriam-webster.com/dictionary/download

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

In this regard, Prof. Miller and Agent Powers agree that while viewing a picture on the Internet (or, for example, "streaming" a movie on Netflix), data related to that content may be temporarily placed in RAM (random access memory). [2] Miller Declaration (dkt. 129, exh. A) at ¶¶ 3(c) and 6; Powers Declaration at ¶ 12. However, "as Professor Miller correctly notes, the contents of RAM are volatile – *i.e.*, they disappear when power is lost – its content must be written to persistent memory, such as the hard drive," in order to be retrievable at a later date. Powers Declaration at ¶ 12. It is the fact that the affiant falsely claimed that the Playpen pictures were stored in long term memory, including the hard drive's "cache," that is the basis of his related false claims that those pictures (and any related data) could be recovered a year later.

In this regard, Powers posits that it is possible that some RAM "artifacts" (like a web site address) could have a longer life span and be recovered with specialized forensic software "under certain circumstances." Powers Declaration at ¶¶ 13-14. But even assuming that is true, and the forensic stars aligned to recover an address or similar "artifact," that is not what the affidavit either claimed or explained. No matter how the Government tries to construe the affidavit, its statements about the storage and recoverability of child pornography are false.

Specifically, if the affidavit meant what it says about pictures and videos being downloaded and stored for many years, then those claims are plainly false because the experts agree that the Tor browser blocks storage in long term or "persistent" memory. *See generally United States v. Romm*, 455 F.3d 990, 993 (9th Cir. 2006) (describing the regular Internet downloading and "cache" storage process that can result in long term data storage and establish a prima facie case of receipt or possession).

---

[2] *See, e.g.*, Chris Welch, The Verge, Nov. 30, 2016, "Netflix finally lets you download shows and movies to watch offline" (describing how Netflix gives users the choice to either "play" a movie or "download" it), available at: http://www.theverge.com/2016/11/30/13792376/netflix-offline-downloads-now-available.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

If alternatively, as the Government may be arguing now, the affidavit's statements about "downloading" instead refer to temporary RAM or "volatile" storage of piecemeal data, like a web address, then the affidavit is still false for two reasons. First, the affidavit did not explain that all this "volatile" data is routinely deleted or overwritten by the computer. Doing so, of course, would have undermined that affidavit's claim that the Playpen pictures or related evidence was likely recoverable a year later. Second, this volatile data, even if it was recoverable, would not include the pictures or videos that the affidavit claims the target was "collecting."

In other words, no matter how the Government slices the affidavit, it turns out to be false when it comes to its representations about where and for how long evidence might be stored. Faced with this dilemma, the Government then tries to minimize the materiality of the false statements by baldly stating that the affidavit "says nothing about where [the Playpen pictures] would be stored or for how long." Govt. Response at 17, l. 24. To the contrary, not only was much of the affidavit directed to persuading the Magistrate Judge that illegal pictures had been sent from Playpen to the target computer, it made a host of assertions about where those images were stored and for how long, including that they would be found "on the user's computer" (Motion to Suppress, exh. B at ¶¶ 33 and 34); that pictures would be retained "for many years" (*id*. at ¶ 43(c)); that downloads "are often maintained for several years" (*id*. at ¶ 43(d)); and that data stored in a computer's hard drive cache "is often maintained indefinitely" (*id*. at ¶ 51).

Nowhere in all of this does the affiant disclose that the pictures were not saved on the computer, or that the Tor browser actively blocks cache saving or similar automatic downloading and long term storage.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

The misleading nature of the affidavit is further revealed by Agent Powers' observation that "TorBrowser allows users to save content with relative ease," by intentionally copying, downloading and saving content with several affirmative "clicks." Powers Declaration at ¶ 15. That fact helps the defense, because the Government does not dispute that the FBI server hosting Playpen would have recorded the affirmative steps that are required to *intentionally* download and save pictures if that had happened. *See* Second Motion to Suppress (dkt. 127) at 3. It was precisely because there was no such evidence of knowing possession or collecting by "candygirl123" that the affidavit was false or misleading in claiming that pictures had been automatically saved in the target computer's long term memory.

The true facts, if they had been disclosed in the affidavit, would have gutted the affiant's efforts to establish probable cause for the Washington search. The falsehoods here are comparable to an affidavit in a drug case where the affiant has claimed that an undercover agent delivered cocaine to the suspect's home, when in fact the delivery never happened. Even if the affidavit alleges that the suspect is a drug user, and there is probable cause to believe that he has consumed cocaine at some time, a warrant that is based on false statements about a drug delivery (let alone false statements about the likelihood of finding those drugs long after the alleged delivery) would inevitably result in suppression.

The fact that this case involves computers rather than drugs makes no difference. Courts have allowed computer searches when the allegations of criminality might otherwise be deemed stale only when an affiant establishes (a) that the suspect received or distributed child pornography, or (b) the affidavit otherwise establishes that the suspect is an actual collector, plus (c) a complete and truthful basis for finding that evidence of receipt or possession can still be found on the target's computer or other

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

devices. And, of course, if there is no evidence that pornography was on the computer to begin with, one never even gets to a staleness analysis.

Thus, in *United States v. Schesso*, 730 F.3d 1040 (9th Cir. 2013) (cited in Govt. Response at 14), the court concluded that a 20 month delay in searching a computer was permissible because the "[k]ey to the probable cause analysis is the evidence that Schesso took the affirmative step of uploading and distributing the video on a network designed for sharing and trading." *Id.* at 1045. The evidence of active sharing of contraband, coupled with a particularized, valid collector profile and long term storage of the evidentiary data, overcame the adverse inferences that might otherwise apply, including the possibility that the suspect merely possessed "a commercial child pornography video, which might have resulted from a onetime accidental download or inadvertent receipt." *Id.*

Here, by contrast, the affidavit did not disclose that the Tor browser blocks the type of automatic downloading that the affidavit relied on to establish receipt and possession in the first place, and it also included a misleading "collector profile." Plainly, if the affidavit had truthfully disclosed not only that "candygirl123" had not downloaded pornography, but also that the Tor browser has unique security features that block downloading, the Magistrate Judge would likely have agreed with the FBI's own Chief Division Counsel that more investigation was required before seeking a warrant.

Finally, the Government does not dispute that Deputy Shook knew or should have known all of the facts relevant to all of the *Franks* issues, including how Tor functions. If there were any doubt about this, the Government has just disclosed (on February 8) email correspondence between Deputy Shook and lead Operation Pacifier Agent Daniel Alfin. Exh. A. As evidenced by these exchanges, Alfin assisted Shook in

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

preparing the local warrant, and even helped edit sections of the affidavit which address the purported downloading of pictures from Playpen.[3]

In short, a reformed affidavit, with the false information about delivery of pornography excised from it, and the true facts about there being no long term storage of Tor content included, affords no basis for concluding that contraband and related data had ever been stored on Mr. Tippens' computer, let alone that it could be found a year later. The affidavit also provides no other grounds for concluding that "candygirl123" was collecting pornography, such as messages or chat on the Playpen site; the posting of pictures on the site; or visits to illegal non-Tor sites (which might have resulted in automatic downloads to cache storage). There is also no doubt that if such evidence had existed it was available to the FBI. The FBI had control of the Playpen server, which contains all of the data related to user activity on the site. The FBI had also identified the Internet Service Provider for the target computer in Hawaii, through which it could have obtained additional information (if it had existed) about illicit Internet activity. No such information was included in the affidavit.

B. The Misleading Collector Profile

With the false statements about automatic downloading and long term storage excised, and the true facts about Tor's security features included, the only arguable basis for concluding that evidence might be found at the Washington residence is the affidavit's "collector profile." The Government's attempt to defend this profile is not persuasive.

The Government first argues that "Tippens does not take issue with Deputy Shook's assertions about child pornography collectors generally." Govt. Response at 19. In fact, the Deputy's "profile" is boilerplate and inconsistent with "expert" collector

[3] As the Court will see, sections of these emails have been redacted. The defense has requested complete and unredacted versions of all correspondence related to the local warrant.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

profiles that the Government has relied on in other cases. *See* Second Motion to Suppress, dkt. 127, at 16 and exh. H (Government expert report in *United States v. Hart*). But more importantly, with no showing that images were ever received, possessed or distributed by "candygirl123," the very characterization of him or her as a "collector" has no factual support, and the profile's attempt to then show that collected images can be retained on a computer becomes irrelevant.

Once the false statements about downloading from Playpen are excised, and the true facts about Tor security are added, all that remains are allegations that a visitor viewed pictures on Playpen a year prior to the search; he or she did not download anything from the site; and the visitor took affirmative measures to avoid saving anything from the site. Those facts are consistent with someone who avoids collecting and are inconsistent with being a collector. And because the profile pertained only to those who act "with intent to view *and* possess, collect, receive, or distribute images of child pornography," the affiant's representation that "candygirl123" fits that profile becomes untenable. Dkt. 129, exh. B (affidavit) at ¶ 43(a) (emphasis added).

The Government's arguments are misguided for the additional reason that Tor users generally are different from "collectors generally." According to the Government itself, Tor users typically behave in security-minded ways that are inconsistent with an intent to collect and the behavior of most other Internet offenders. Accordingly, when the Government wanted to persuade the court in Eastern Virginia that the Playpen investigation was time sensitive and justify delaying the notices otherwise required by Fed. R. Crim. P. 41, it maintained that Tor users are more technologically sophisticated than the average Internet offender, adept at security and avoiding detection, and likely to delete or destroy evidence. *See, e.g.*, Second Motion to Suppress (dkt. 127) at 9; dkt. 129, exh F, at 416, 423 and 431.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

This is not, then, a question of a few "exceptions" to a "rule of thumb." *See* Govt. Response at 21. Rather, it is a question of different classes of people who behave quite differently, with "candygir123" belonging to one group and the affiant discussing another. Worse yet, the Government has several times alleged that Operation Pacifier searches were time sensitive because of the nature of Tor and its users, only to omit all of that information from the local warrant application and make inconsistent claims about how evidence was likely to linger for years.

The Court should not allow the Government to have it both ways. The only reason not to have included the relevant characteristics in the instant "profile" is because they are plainly inconsistent with the conclusions that the affiant needed the Magistrate Judge to reach in order to find that a search was still timely. As a result, Deputy Shook not only failed to "specifically identif[y] the circumstances linking the collector profile' to 'candygirl123,'" as the Government claims, he omitted from the profile all of the facts that did not fit. *See* Govt. Response at 20 (quoting *United States v. Gourde*, 440 F.3d 1065, 1074 (9th Cir. 2006). That alone was a *Franks* violation.

With a reformed affidavit, in which the profile is excised and the true facts about Tor users are included, there is no legitimate basis for concluding that any illegal pictures or related data would be retained "for several years," as the profile expressly alleges. Second Motion to Suppress (dkt. 127), exh. B at ¶ 43(d).

C. The Lack of Nexus Between the Time and Place of the Alleged Viewing and the Search.

What distinguishes this case from *United States v. Gourde* are the numerous facts there that overcame any concerns about staleness, while here the affidavit relies on a boilerplate and misleading collector profile to overcome such concerns. *See* Govt. Response at 10.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

In *Gourde*, the court emphasized that the affidavit established that the defendant had paid for a continuing membership to a pornography site, thereby supporting the inference that Gourde was seeking something of value to him and was therefore likely to keep what he had paid for. 440 F.3d at 1070. Gourde had also taken the affirmative steps of providing personal and credit card information for that membership. In this case, the FBI was distributing its pornography for free to at least 100,000 visitors, and anyone who came across Playpen could access and view its content without receiving anything.

In addition, *Gourde* involved the regular Internet; explicit child pornography that was posted on the site's home page and elsewhere would have been automatically downloaded and stored on his computer, supporting the conclusion that the contraband "would remain on the computer for an extended time." *Id*. at 1068.

Here, by contrast, the affidavit misled the court about the target receiving and storing pictures from Playpen, and if the true facts had been disclosed there would have been no basis to conclude that pornography was ever on the "candygirl123" computer. Gourde also continuously resided at the house where he had maintained his membership, and the warrant was executed just four months after the site was shut down, two facts sharply in contrast to this case. *Id.* at 1067-68.

The Government's reliance on *Schesso* and several cases from other circuits is equally misplaced. Govt. Response at 14-15. In fact, *Schesso* supports a suppression order in this case. The Court is already familiar with the case, having granted Mr. Schesso's motion to suppress. Notably, the Court stated in its oral ruling that "when there is a delay [in obtaining a search warrant], it enhances the need for narrowness and for tying the defendant into a continuing course of conduct that becomes more important as time goes on." *United States v. Schesso*, CR11-05285RJ, dkt. 88 at 47.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

On appeal, Schesso did not even challenge probable cause to search his computers, the issue instead being "the lack of any guidance or limits in the warrant for subsequently searching the intermingled data that was on them." 730 F.3d at 1045. Moreover, the affidavit in *Schesso* established that he was using a peer-to-peer file sharing program that is often used to distribute pictures and, most importantly, that he had in fact distributed child pornography. *Id.* Hence, there was probable cause to believe that Schesso not only possessed child pornography but was engaged in a "continuing pattern" of collecting and distributing. In this case, however, the affidavit falsely alleged that "candygirl123" had received child pornography, and it contained no other facts showing possession, distribution, or any continuing pattern of activity that extended from Hawaii to University Place.

Further, *Schesso* did not involve Tor; the affidavit accurately explained that the computer programs that were involved in the case would retain pictures and videos indefinitely. Here, the affidavit concealed the facts about Tor's security features and falsely claimed that the Playpen pictures, which were never stored in the first place, would be retained for years.

The *Schesso* collector profile was also both particularized and accurate, and it did not omit inconsistent information. Specifically, the Ninth Circuit found that, "[b]ased on the evidence that Schesso possessed and distributed a child pornography video on a peer-to-peer file-sharing network, law enforcement agents had probable cause to believe that Schesso was a child pornography collector and thus to search Schesso's computer system for any evidence of possession of or dealing in child pornography." *Id*. at 1049. Here, the affidavit not only made false representations about the target's downloading and possession of child pornography, it excluded from the profile all the relevant propensities of Tor users.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

In addition, Schesso not only continuously resided at the location from which he had distributed pornography, the affidavit established that he was still active on the Internet at that location not long before the police sought a warrant. CR11-05285RJ, dkt. 64-1 (warrant application) at ¶ 30 (stating that the police used a portable "Cantenna" device "to search for available [Internet] networks that were broadcasting in the area" of Mr. Schesso's home and establishing that he had Internet service). Here, a prolonged temporal gap is coupled with a vast physical gap between the location of alleged criminality and the search, with no continuing activity of any kind to connect the two. *Cf. United States v. Coon*, 2011 WL 1871165 (W.D.N.Y. May 16, 2011) (where child pornography was affirmatively shown to be on user's home computer, but there was no showing that that computer was likely to still be possessed a year later, probable cause was lacking).[4] As a result, the affidavit not only fails to establish a nexus between the alleged crime and the search location, it omitted information (the moving inventory) that weighs against finding a nexus.

In short, *Schesso* is not helpful to the Government because it contains a virtual laundry list of the types of information that an affidavit should contain in order to establish a continuing pattern or other good reason to believe that digital evidence will be found after a prolonged lapse of time. It is undisputed that when an affidavit contains truthful allegations establishing probable cause to believe that a suspect received or distributed child pornography, and also includes a particularized collector profile that establishes that the suspect is in fact a likely collector, those facts can compensate for otherwise stale information. But the problem here is that the affidavit makes no showing that "candygirl123" was a collector; it omitted all of the information about the

[4] The *Coon* court found the good faith exception applicable, given that there were no *Franks* violations or other factors taking the case outside the scope of that exception. 2011 WL 1871165, at *5. As discussed in the Mr. Tippens' Second Motion to Suppress at 10 and 24-26, the good faith doctrine is not applicable in this case.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Tor network that is inconsistent with collecting; it falsely claimed that the target had stored child pornography on his computer; and it offered no other reason for concluding that any evidence that might have existed in Hawaii could be later found in Washington.

Finally, the cases from other circuits that the Government has cited are similar to *Schesso* and have little or no relevance here. *See* Govt. Response at 15. For example, in *United States v. Allen*, 625 F.3d 830 (5th Cir. 2010), the defendant also belonged to a file sharing network on the regular Internet, and the affidavit established that the defendant had actually sent pornographic pictures from his home, thereby supporting the conclusions that he not only possessed contraband but that it would still be found on his computer. *Id*. at 841.

Similarly, in *United States v. Seiver*, 692 F.3d 774, 775 (7th Cir. 2012), the warrant application truthfully established that a child pornography video had been downloaded at the defendant's home, and also that a related message had been sent from the same location to the mother of the victim. In reviewing these facts, the court zeroed in on one of the key issues here, namely "the importance to a determination of 'staleness' of whether the suspect was a 'collector' and thus likely to have 'retained' or 'maintained" rather than 'destroyed' the pornographic images that he had acquired." *Id*. at 775. The court then focused on whether picture or videos, once an affidavit has established their presence on a computer, can ever be fully deleted. *Id.* at 777.

Here, by contrast, the affidavit falsely claimed that "candygirl123" had received pictures in the first place. The affidavit also offered no other basis for concluding that the target possessed contraband or was a collector; it failed to disclose that the available facts indicated that Mr. Tippens had not taken a computer to Washington; and it offered no basis for concluding that he otherwise had a computer or was accessing the Internet near the time of the search.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

IV. CONCLUSION

The defense has already anticipated and addressed the Government's reliance on the good faith doctrine. *See* Govt. Response at 24-26; Second Motion to Suppress (dkt. 127) at 10, 24-26. Accordingly, for the reasons set forth in Mr. Tippens' Second Motion to Suppress and this Reply, the Court should either suppress the fruits of the warrant or first grant a *Franks* hearing, after which it should suppress.

DATED this 9th day of February, 2017.

Respectfully submitted,

s/ *Colin Fieman*
Colin Fieman
Attorney for David Tippens

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

CERTIFICATE OF SERVICE

I hereby certify that on February 9, 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

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Miller, Emily (USAWAW)

From: Doug Shook [redacted]
Sent: Friday, January 29, 2016 8:53 AM
To: Alfin, Daniel I. (CID) (FBI)
Subject: RE: tippens

Thank you! I really appreciate the info. I get a bit hesitant testifying to what a person may have seen when I don't even know what the website looked like. I know you sent the general case info in the cd, but that is still different than visiting the site itself and understanding what is displayed on each posting screen or sub-menu.

Thank you again.
Doug Shook

For future reference; do you prefer going by Dan, Daniel, or Alfin?

From: Alfin, Daniel I. (CID) (FBI) [redacted]
Sent: Friday, January 29, 2016 5:55 AM
To: Doug Shook [redacted]; Hampton, Matthew (USAWAW) [redacted]
Subject: RE: tippens

Matt, Doug, I have the following suggestions for the affidavit. [redacted]

[redacted]

I suggest the following revised language for paragraph 30-

On February 28, 2015, the user "candygirl123" with IP address 66.8.138.192 accessed the post titled, "Latina Anal Part 1 & 2" which was located in the "Pre-teen Videos", "Girls HC" section of "Website A". This post contained a set of 38 embedded images that depicted what appeared to be a prepubescent female engaged in oral, anal penetrative sexual activity with an adult male. The images were embedded in the post such that they would have been downloaded to the user's computer and displayed on the user's computer screen upon accessing the post.

I suggest the following revised language for paragraph 32-

On February 26, 2015, the user "candygirl123" accessed the post titled, "Re: Requested: 8yo fox", which was located in the "Pre-teen Photos", "Girls HC" section of "Website A". This post contained 2 embedded images that depicted a nude prepubescent female. In one image the prepubescent female is depicted sitting on a bed with her legs spread and her nude genitals exposed to the camera. The second image depicts the nude prepubescent female with her hands "hogtied" together with a rope. The prepubescent female's nude genitals and anus are exposed to the camera. The images were embedded in the post such that they would have been downloaded to the user's computer and displayed on the user's computer screen upon accessing the post.

I suggest the following revised language for paragraph 33-

Exhibit A-1
TIPPENS_001008

On February 28, 2015, the user "candygirl123" accessed the post entitled, "Kait aka Sugar" which was located in the "Pre-teen Videos", "Girls HC" section of "Website A". This post contained an embedded image that was a compilation of 240 individual images that depicted what appeared to be prepubescent females engaged in oral and vaginal penetrative sexual activity with adult males. Some of the prepubescent females depicted appeared to be toddler age. The image was embedded in the post such that it would have been downloaded to the user's computer and displayed on the user's computer screen upon accessing the post. Additionally, after accessing the post, the user clicked directly on the described image which would have resulted in downloading another copy of the image to the user's computer.

From: Doug Shook
Sent: Thursday, January 28, 2016 7:51 PM
To: Hampton, Matthew (USAWAW)
Cc: Alfin, Daniel I. (CID) (FBI)
Subject: RE: tippens

Matt and Daniel,

I made corrections on some of the identified tabs. Daniel, is there any way you or your team can address some of the questions Matt has identified for the material provided by your team in the initial investigation? I really don't like to pass the work off, but I do not have the information to properly answer the issues.

And as always –when it comes to someone asking for things like this- any kind of rush that could be put on this would be greatly appreciated so that we can beat the February 8th deadline for the general notification that is reportedly going to occur.

Doug Shook
cell

From: Hampton, Matthew (USAWAW)
Sent: Thursday, January 28, 2016 4:10 PM
To: Doug Shook
Subject: tippens

Doug,

Give me a call tomorrow if you have time. (or today, I'll be here until around 5.)

Exhibit A-2
TIPPENS_001009

MATTHEW P. HAMPTON
Assistant United States Attorney
United States Attorney's Office
Western District of Washington
700 Stewart Street, Suite 5220
Seattle, Washington 98101
Direct:
Cell