

1 **WO**

2

3

4

5

6

IN THE UNITED STATES DISTRICT COURT

7

FOR THE DISTRICT OF ARIZONA

8

9 United States of America,

No. CR-17-01311-001-PHX-DGC

10

Plaintiff,

11

v.

12

Anthony Espinoza Gonzales,

13

Defendant.

14

15 United States of America,

No. CR-18-00539-001-PHX-DGC

16

Plaintiff,

17

v.

ORDER

18

Aaron Anthony Ordonez,

19

Defendant.

20

21

22

Defendants Anthony Espinosa Gonzales and Aaron Ordonez are charged in two separate cases with distributing and possessing child pornography in violation of 18 U.S.C. § 2252(a). Each has filed a motion to compel disclosure of the Torrential Downpour software program used by the FBI in the investigation that led to his indictment. Doc. 25, Case No. CR-17-01311; Doc. 32, Case No. CR-18-00539. Both motions are fully briefed, and the Court held a joint evidentiary hearing on January 31, 2019. Computer forensics expert Tami Loehrs testified on behalf of Defendant Gonzalez,

23

24

25

26

27

28

1 and FBI Agent Jimmie Daniels testified for the government. The Court will grant
2 Defendant Gonzalez's motion in part and deny it in part, and will deny Defendant
3 Ordonez's motion.

4 **I. Background.**

5 **A. The BitTorrent Network and Torrential Downpour.**

6 The indictments in these cases allege that Defendants downloaded and shared
7 child pornography files using the BitTorrent file-sharing network. BitTorrent is an online
8 peer-to-peer network that allows users to download files containing large amounts of
9 data, such as movies, videos, and music. Instead of relying on a single server to provide
10 an entire file directly to another computer, which can cause slow download speeds,
11 BitTorrent users can download portions of the file from numerous other BitTorrent users
12 simultaneously, resulting in faster download speeds.

13 To download and share files over the BitTorrent network, a user must install a
14 BitTorrent software "client" on his computer and download a "torrent" from a torrent-
15 search website. A torrent is a text-file containing instructions on how to find, download,
16 and assemble the pieces of the image or video files the user wishes to view. The client
17 software reads the instructions in the torrent, finds the pieces of the target file from other
18 BitTorrent users who have the same torrent, and downloads and assembles the pieces,
19 producing a complete file. The client software also makes the file accessible to the other
20 BitTorrent users in a shared folder on the user's computer.

21 Torrential Downpour is law enforcement's modified version of the BitTorrent
22 protocol. Torrential Downpour acts as a BitTorrent user and searches the internet for
23 internet protocol ("IP") addresses offering torrents containing known child pornography
24 files. When such an IP address is found, the program connects to that address and
25 attempts to download the child pornography. The program generates detailed logs of the
26 activity and communications between the program and the IP address. Unlike traditional
27 BitTorrent programs, the government claims that Torrential Downpour downloads files
28 only from a single IP address – rather than downloading pieces of files from multiple

1 addresses – and does not share those files with other BitTorrent users.

2 **B. The Investigations into Defendants’ BitTorrent Activity.**

3 **1. Defendant Gonzales.**

4 In December 2016, Agent Daniels used Torrential Downpour to identify IP
5 address 24.255.44.200, which allegedly was making known child pornography files
6 available on the BitTorrent network. Agent Daniels testified that he used Torrential
7 Downpour to connect with this IP address and download child pornography video files on
8 eight occasions between December 13, 2016 and January 9, 2017. He reviewed the
9 Torrential Downpour activity logs to confirm that the program downloaded complete
10 files solely from this IP address, and reviewed the video files to confirm that they were
11 child pornography.

12 Through further investigation, Agent Daniels learned the subscriber information
13 for the IP address. He obtained a search warrant for the subscriber’s residence, and FBI
14 agents searched the residence on February 8, 2017. They found a Microsoft tablet and
15 other computer equipment. Gonzales, who lived there with his parents and siblings,
16 stated during an interview that he had used a tablet to find and view child pornography.
17 Forensic examinations performed by the FBI and Loehrs revealed child pornography files
18 on the tablet, but the video files that Torrential Downpour allegedly had downloaded
19 from the IP address were not found on the tablet or any other seized device.

20 On October 4, 2017, the government charged Gonzales with eight counts of
21 distributing child pornography and one count of possessing such material. Doc. 6.
22 The eight distribution counts are based on the video files that Torrential Downpour
23 allegedly downloaded between December 13, 2016 and January 9, 2017. *Id.* at 1-5. The
24 possession count is based on the child pornography found on the tablet after the search.
25 *Id.* at 5-7.

26 **2. Defendant Ordonez.**

27 Agent Daniels conducted a similar investigation into Defendant Ordonez’s
28 BitTorrent activity. On five occasions between December 2, 2017 and February 5, 2018,

1 Agent Daniels used Torrential Downpour to connect with and download child
2 pornography files from IP address 24.251.70.98. The FBI obtained a search warrant for
3 the residence associated with that IP address, and seized Ordonez’s computer during a
4 search on April 4, 2018. The FBI performed a forensic examination of the computer and
5 found thousands of child pornography files in the recycle bin, including the files
6 Torrential Downpour had downloaded. On April 17, 2018, the government charged
7 Ordonez with five counts of distributing child pornography and one count of possessing
8 such material. Doc. 10.

9 **II. Discussion.**

10 Defendants contend that Torrential Downpour may be flawed and should be tested
11 and verified by a third party. They also contend that they need access to the program in
12 order to prepare effective cross examination of Agent Daniels and the presentations by
13 their own computer experts. Defendants seek disclosure of an installable copy of the
14 software pursuant to Federal Rule of Criminal Procedure 16, *Brady v. Maryland*, 373
15 U.S. 83 (1963), and *Giglio v. United States*, 405 U.S. 150 (1972). Gonzales also seeks
16 disclosure of Torrential Downpour’s user and training manuals. Neither Defendant seeks
17 the program’s source code.

18 The government contends that Defendants have failed to show how Torrential
19 Downpour is material to their defense. The government further contends that even if
20 materiality has been shown, Torrential Downpour is protected from disclosure by the
21 qualified law enforcement privilege recognized in *Roviaro v. United States*, 353 U.S. 53
22 (1957).

23 **A. Rule 16(A)(1)(E)(i) – Items Material to Preparing a Defense.**

24 Under Rule 16(a)(1)(E), the government must disclose any “books, papers,
25 documents, data, . . . or portions of any of these items, if the item is within the
26 government’s possession, custody, or control and: (i) the item is material to preparing the
27 defense[.]” To obtain disclosure under subsection (i), “[a] defendant must make a
28 ‘threshold showing of materiality[.]’” *United States v. Budziak*, 697 F.3d 1105, 1111 (9th

1 Cir. 2012) (citing *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir. 1995)). “Neither
2 a general description of the information sought nor conclusory allegations of materiality
3 suffice; a defendant must present *facts* which would tend to show that the [g]overnment is
4 in possession of information helpful to the defense.” *United States v. Mandel*, 914 F.2d
5 1215, 1219 (9th Cir. 1990) (emphasis added); *see also Budziak*, 697 F.3d at 1111-12.

6 **1. Discoverability of Investigative Software.**

7 Many cases have addressed the discoverability of government software programs
8 used to investigate child pornography offenses. The parties each cite lines of cases to
9 support their positions.

10 Defendants rely primarily on *United States v. Budziak*, 697 F.3d 1105 (9th Cir.
11 2012), and cases that have adopted its reasoning. *Budziak* involved the FBI’s use of an
12 enhanced version of the LimeWire file-sharing program called “EP2P.” *Id.* at 1107.
13 Using that program, the FBI downloaded several child pornography files from an IP
14 address registered to Budziak. *Id.* A forensic examination of his computer revealed
15 multiple child pornography files, including several images the EP2P program had
16 downloaded. *Id.* Budziak was charged with multiple counts of distributing and
17 possessing child pornography. *Id.* The district court denied Budziak’s motions to
18 compel disclosure of the government’s EP2P program, and he was convicted on each
19 count. *Id.* at 1107-08.

20 On appeal, the Ninth Circuit held that the district court abused its discretion in
21 denying Budziak’s motions to compel. It noted that he did more than assert a generalized
22 need to review the EP2P program before trial; he identified particular defenses to the
23 distribution charges that discovery on the EP2P program could help him develop. *Id.*
24 at 1112. Specifically, he “presented evidence suggesting that the FBI may have only
25 downloaded fragments of child pornography files from his ‘incomplete’ folder, making it
26 ‘more likely’ that he did not knowingly distribute any complete child pornography files
27 to [the FBI].” *Id.* at 1112. He also presented “evidence suggesting that the FBI agents
28 could have used the EP2P software to override his sharing settings.” *Id.* Given this

1 evidence, the Ninth Circuit concluded that “access to the EP2P software was crucial to
2 Budziak’s ability to assess the program and the testimony of the FBI agents who used it
3 to build the case against him.” *Id.*

4 Other cases have followed *Budziak*. For example, the district court in *United*
5 *States v. Crowe*, No. 11 CR 1690 MV, 2013 WL 12335320, at *7 (D.N.M. Apr. 3, 2013),
6 required the government to allow the defense expert to examine and use a copy of the
7 government’s confidential Shareaza software at a secure government facility. The court
8 did so because the defendant in *Crowe*, like the defendant in *Budziak*, presented specific
9 evidence to suggest that access to the software was material to preparing the defense.
10 *See id.* Specifically, the defense expert testified that “some of the files alleged to have
11 been found by law enforcement in the shared space of Defendant’s computer, were not
12 found there during her analysis.” *Id.*

13 Another line of cases has refused to permit defendants in child pornography cases
14 to gain access to confidential government investigative software. In *United States v.*
15 *Pirosko*, 787 F.3d 358 (6th Cir. 2015), a case cited by the government in response to
16 these motions, the court of appeals affirmed a district court decision denying discovery of
17 the “law enforcement tools” used to locate and download child pornography from the
18 defendant’s computer. The Sixth Circuit distinguished *Budziak*, noting that the defendant
19 in that case had presented the evidence described above. 787 F.3d at 365-67. The
20 defendant in *Pirosko*, by contrast, “failed to produce any such evidence, simply alleging
21 that he might have found such evidence had he been given access to the government’s
22 programs.” *Id.* at 365. As a result, discovery was not warranted. *Id.*

23 Other cases have likewise found that the defendant in child pornography cases has
24 failed to make a showing to support their claim that disclosure of government
25 investigative software would be material to preparing the defense. *See United States v.*
26 *Jean*, 891 F.3d 712, 715 (8th Cir. 2018) (affirming denial of motion to compel
27 government software because the defendant was convicted of receiving and possessing
28 child pornography and “the likelihood of any help to [his] defense was ‘vanishingly

1 small”); *United States v. Chiaradio*, 684 F.3d 265, 277 (1st Cir. 2012) (expressing no
2 view on whether the EP2P source code was discoverable under Rule 16 where the
3 defendant “neither contradicted nor cast the slightest doubt upon” the government’s
4 evidence that the FBI had downloaded child pornography from his computer); *United*
5 *States v. Hoeffener*, No. 4:16-CR-00374, 2017 WL 3676141, at *13 (E.D. Mo. Aug. 25,
6 2017) (denying motion to compel where “nothing in the . . . receipt-of-child-pornography
7 charge reveal[ed] that the charge [was] based, to any extent, on materials downloaded
8 from [the defendant’s] computer while [the FBI] used Torrential Downpour”); *United*
9 *States v. Blouin*, 2017 WL 2573993, at *3 (W.D. Wash. June 14, 2017) (denying motion
10 to compel where the defendant did not dispute that the government’s software downloads
11 files from a single source); *United States v. Maurek*, No. CR-15-129-D, 2015 WL
12 12915605 at *3 (W.D. Okla. Aug. 31, 2015) (denying motion to compel where the
13 defendant failed to present specific facts which would tend to show how disclosure of
14 Torrential Downpour would be material to his defense); *United States v. Feldman*, No.
15 13-CR-155, 2015 WL 248006, at *6 (E.D. Wis. Jan. 19, 2015) (finding a lack of
16 materiality where the defendant was charged with receiving and possessing child
17 pornography based on a search of his computer and not the use of the government’s
18 software).

19 *Budziak* is, of course, binding precedent for this Court. But the Court finds the
20 distinction between it and the cases just discussed to be consistent with traditional
21 Rule 16 principles. As already noted, “[n]either a general description of the information
22 sought nor conclusory allegations of materiality suffice [under Rule 16(a)(1)(E)(i)]; a
23 defendant must present *facts* which would tend to show that the [g]overnment is in
24 possession of information helpful to the defense.” *Mandel*, 914 F.2d at 1219 (emphasis
25 added). In *Budziak* and *Crowe*, the defendants presented evidence to support their
26 contention that discovery of the government software was material to preparing their
27 defense to distribution of child pornography. In the other line of cases, they did not. The
28 Court will keep this distinction in mind as it considers the arguments of Defendants

1 Gonzalez and Ordonez.

2 **2. Gonzales Has Shown Materiality.**

3 Counts one through eight allege violations of 18 U.S.C. § 2252(a)(2). Doc. 1.
4 That section provides criminal punishment for any person who “knowingly receives, or
5 distributes, any visual depiction using any means or facility of interstate or foreign
6 commerce . . . including by computer, . . . if (A) the producing of such visual depiction
7 involves the use of a minor engaging in sexually explicit conduct; and (B) such visual
8 depiction is of such conduct[.]” Evidence is sufficient to support a conviction for
9 distribution under § 2252(a)(2) “when it shows that the defendant maintained child
10 pornography in a shared folder, knew that doing so would allow others to download it,
11 and another person actually downloaded it.” *Budziak*, 697 F.3d at 1109.

12 Defendant Gonzales argues that Torrential Downpour is material to his defense
13 because the distribution charges are based on child pornography files that Torrential
14 Downpour purportedly downloaded from his tablet but that were not found on the tablet
15 when it was seized by the FBI. Doc. 25 at 8-9. He has presented an affidavit from his
16 expert, Tami Loehrs, confirming that the files are not on the tablet. Doc. 25-5. Loehrs
17 explains in her affidavit that it is critical to Gonzales’s defense to understand how
18 Torrential Downpour functions in order to determine the program’s reliability and
19 accuracy in identifying files that Gonzales is charged with knowingly distributing. *Id.*
20 at ¶ 17. She further states that based on her many years of research and testing of peer-
21 to-peer file sharing software, including BitTorrent, she has discovered that all of these
22 programs “contain bugs, they do not always function as intended and the data reported by
23 these applications is not always accurate or reliable.” *Id.* ¶ 22.

24 Loehrs offered similar opinions at the evidentiary hearing. She opined that all
25 software programs have flaws, and Torrential Downpour is no exception. *See* Doc. 50,
26 Hr’g Tr. at 16:15-23, 18:17-19, 31:6-10 (Jan. 31, 2019). She bases this opinion on her
27 work in other cases involving Torrential Downpour and the fact that the files the program
28 allegedly downloaded in this case were not found on Gonzales’s tablet. *Id.* at 16:1-23.

1 Loehrs also provided a plausible explanation for how Torrential Downpour may
2 have erroneously identified Gonzales’s tablet as offering child pornography files over the
3 BitTorrent network. Loehrs explained that, because a torrent is simply a text-file
4 containing the hash values – or “fingerprints” – of the target image and video files, a
5 BitTorrent user who downloads a torrent has fingerprints of the target files, even if he has
6 not yet downloaded them. *Id.* at 22:14-23:8. Loehrs stated that the actual downloading
7 of the target files occurs only when the client software instructs the torrent to search for
8 those files on the BitTorrent network and download them to a designated folder on the
9 user’s computer. *Id.* at 23:9-25:3. She further stated that a forensic examination of the
10 device used to download the torrent can determine whether the torrent has been used to
11 download the file, and her examination of Gonzales’s tablet revealed no evidence
12 suggesting that he downloaded the files listed in counts one through eight. *Id.* at 25:4-22,
13 28:7-9. She opined that Torrential Downpour may have obtained the files from other
14 BitTorrent users, particularly in light of the fact that this is how peer-to-peer file sharing
15 programs are designed to work. *Id.* at 31:3-32:12.¹

16 The Court finds that this evidence brings this case squarely within the holding of
17 *Budziak*. Defendant Gonzalez has done more than simply request access to the software
18 and argue that it is material to his defense. He has presented evidence that calls into
19 question the government’s version of events. Given his evidence, the Court finds that
20 “the functions of the [program] constitute[] a ‘very important issue’ for [Gonzales’s]
21 defense.” *Budziak*, 697 F.3d at 1112 (quoting *United States v. Cedano-Arellano*, 332
22 F.3d 568, 571 (9th Cir. 2003)); *see Crowe*, 2013 WL 12335320, at *7.²

23 The government concedes that the child pornography files charged in counts one
24

25 ¹ The government contends that Loehrs’s affidavit is unreliable, citing several
26 cases rejecting or limiting the scope of her testimony. Doc. 29 at 5, 20-22. The Court
27 found Loehrs credible at the evidentiary hearing and has no basis at this point for
excluding her opinions under Federal Rule of Evidence 702.

28 ² Gonzales asserts that the government’s need to present evidence of Torrential
Downpour in its case-in-chief also entitles him to discovery under Rule 16(a)(1)(E)(ii),
but he fails to develop this argument or cite relevant case law.

1 through eight were not found on Gonzales’s tablet. Doc. 29 at 3. The government notes,
2 however, that torrent names associated with these files were located in a “µTorrent”
3 client software folder on the tablet, that some of these torrent names were in a
4 “jump list,” which suggests that Gonzalez had clicked on them, and that other child
5 pornography files were found on the tablet. *Id.* at 13. Materiality is defeated, the
6 government contends, because these facts corroborate its claim that Gonzales once
7 possessed the files charged in counts one through eight and was able to distribute them to
8 the FBI. *Id.* at 17.

9 But where a defendant has demonstrated materiality, the Court “should not merely
10 defer to government assertions that discovery would be fruitless.” *Budziak*, 697 F.3d
11 at 1112-13. While the Court has no reason to doubt the government’s good faith in this
12 case, Gonzales “should not have to rely solely on the government’s word that further
13 discovery is unnecessary.” *Id.* at 1113. Because Gonzales has shown that the Torrential
14 Downpour is material to his defense, he should be given access to the program to
15 investigate its reliability and help him prepare for cross-examination of Agent Daniels.³

16 Gonzales also contends that Torrential Downpour is material to a Fourth
17 Amendment challenge because the program “searches beyond the public domain,
18 essentially hacks computers searching for suspect hash values, and therefore conducts a
19 warrantless search[.]” Doc. 25 at 6. But Gonzales identifies no evidence suggesting that
20 Torrential Downpour accessed non-public space on his tablet. Gonzales has failed to
21 show that Torrential Downpour is material to a Fourth Amendment challenge. *See*
22 *Hoeffener*, 2017 WL 3676141, at *15 (finding a lack of materiality where the defendant
23 pointed to no “aspects of his expert’s declaration that support his request for information
24 based on a search warrant challenge”).

25
26 ³ The government presents a log file purportedly showing that Agent Daniels used
27 Torrential Downpour to download from Gonzales’s tablet the child pornography file
28 listed in count four. Doc. 29-2; *see* Doc. 6 at 3. The government asserts that this log file
and the ones associated with the other distribution counts independently confirm that
Agent Daniels downloaded complete child pornography files solely from Gonzales’s
tablet. Doc. 29 at 26. But the log files were created by Torrential Downpour. If it is
flawed in the ways Gonzales suggests, they likely would be flawed as well.

3. Ordonez Has Failed to Show Materiality.

1
2 Defendant Ordonez asserts that it is critical to understand how Torrential
3 Downpour functions “to determine its reliability and accuracy in identifying files
4 reported[ly] involving [his] IP address and whether law enforcement went beyond
5 accessing information that was publicly available.” Doc. 32 at 3. But Ordonez has
6 identified no “specific defense to the charges against him that the Torrential Downpour
7 program could help him develop.” *Maurek*, 2015 WL 12915605 at *3. Nor has he
8 presented any evidence in support of this materiality argument. Conclusory allegations
9 of materiality are not sufficient to compel disclosure under Rule 16(a)(1)(E)(i). *See*
10 *Budziak*, 697 F.3d at 1111-12 (citing *Mandel*, 914 F.2d at 1219); *Santiago*, 46 F.3d
11 at 894-95 (the defendant’s “assertions, although not implausible, do not satisfy the
12 requirement of specific facts, beyond allegations, relating to materiality”).

13 Defendant Ordonez does argue in his motion that his expert needs access to
14 Torrential Downpour to determine its reliability. Doc. 32 at 2. He clarified in his reply
15 brief that an associate with Loehrs’s firm, Michele Bush, is his defense expert. Doc. 45
16 at 4. Bush apparently was retained by Ordonez’s former counsel and prepared a report of
17 her examination of Ordonez’s computer in July 2018, but the report has not been
18 disclosed to the government and has not been provided to the Court. *See* Doc. 43 at 2
19 & n.1. Nor did Defendant Ordonez present an affidavit from Bush to support his motion,
20 or call Bush to testify at the evidentiary hearing. Loehrs testified at the hearing that her
21 firm is no longer working on Defendant Ordonez’s case and she has no familiarity with
22 the FBI’s investigation in that case. Doc. 50 at 58:3-7. Ordonez’s counsel stated that he
23 intends to engage another expert going forward (*id.* at 169:5-6), and he cross-examined
24 Agent Daniels at the hearing, but he has presented no case-specific expert evidence to
25 support the motion to compel.

26 Because Defendant Ordonez has failed to make a threshold showing of materiality
27 under Rule 16(a)(1)(E)(1), his case falls within the line of cases that distinguish *Budziak*
28 and deny discovery of government investigative software. *See Pirosko*, 787 F.3d at 366

1 (the defendant’s mere allegation that there were unanswered questions about the
2 government’s software was not sufficient to show materiality); *Maurek*, 2015 WL
3 12915605, at *3 (denying motion to compel disclosure of Torrential Downpour where the
4 defendant offered nothing more than conclusory allegations of materiality); *United States*
5 *v. Alva*, No. 2:14-cr-00023-RCJ-NJK, 2018 WL 327613, at *2 (D. Nev. Jan. 8, 2018)
6 (distinguishing *Budziak* where the defendant presented no evidence that he did not store
7 child pornography in shared folders and made no showing that his “theory behind
8 requesting the RoundUp source code amount[ed] to anything more than an abstract
9 possibility”); *United States v. Harney*, No. CR-16-38-DLB-CJS, 2018 WL 1145957,
10 at *6 (E.D. Ky. Mar. 1, 2018) (finding that the defendant’s arguments in support of his
11 need for the software were closer to *Pirosko* than *Budziak* because he “merely alleged he
12 might find evidence in support of his defense if his expert [was] provided the opportunity
13 to analyze the requested information in its entirety”).

14 **B. *Brady and Giglio.***

15 Defendants also seek disclosure of Torrential Downpour under *Brady v. Maryland*,
16 373 U.S. 83 (1963), and *Giglio v. United States*, 405 U.S. 150 (1972). “The *Brady*
17 standard for materiality is higher than Rule 16’s, and its scope narrower.” *United States*
18 *v. Pac. Gas & Elec. Co.*, No. 14-cr-00175-TEH, 2016 WL 3185008, at *2 (N.D. Cal.
19 June 8, 2016). Under *Brady*’s constitutional mandate, the government “is obligated by
20 the requirements of due process to disclose material exculpatory evidence on its own
21 motion, without request.” *Carriger v. Stewart*, 132 F.3d 463, 479 (9th Cir. 1997). Under
22 *Giglio*, the government’s obligation to disclose exculpatory evidence was expanded to
23 include information that could be used to impeach government witnesses. *See Giglio*,
24 405 U.S. at 154.

25 But it is the government, not the defendant or the trial court, that decides
26 prospectively what information, if any, is exculpatory and must be disclosed under *Brady*
27 and *Giglio*. *See United States v. Lucas*, 841 F.3d 796, 807 (9th Cir. 2016). “The
28 *Brady/Giglio* doctrine does not require the government to disclose neutral . . . evidence.”

1 *United States v. Correia*, No. 2:17-CR-00001-JAD-CWH, 2018 WL 3416517, at *2 (D.
2 Nev. July 9, 2018) (citing *United States v. Stinson*, 647 F.3d 1196, 1208 (9th Cir. 2011)).
3 Defendants have made no showing that Torrential Downpour will prove to be
4 exculpatory or could be used to impeach a government witness. The Court will deny
5 Defendants' motions to the extent they seek disclosure of Torrential Downpour under
6 *Brady* and *Giglio*.

7 This ruling is not inconsistent with Gonzales's showing of materiality under
8 Rule 16 because "[i]nformation that is not exculpatory or impeaching may still be
9 relevant to developing a possible defense." *United States v. Muniz-Jaquez*, 718 F.3d
10 1180, 1183 (9th Cir. 2013). Indeed, "[e]ven inculpatory evidence may be relevant
11 [because a] defendant who knows that the government has evidence that renders his
12 planned defense useless can alter his trial strategy [or] seek a plea agreement instead of
13 going to trial." *Id.*; see also *United States v. Toilolo*, No. CR-11-00506-LEK, 2014 WL
14 1091715, at *3 (D. Haw. Mar. 17, 2014) ("Rule 16 is broader than *Brady*, 'requiring
15 disclosure of all documents material to preparing the defense.'" (quoting *Muniz-Jaquez*,
16 718 F.3d at 1183)).

17 **C. The Qualified Law Enforcement Privilege Under *Roviaro*.**

18 Even when a defendant is entitled to disclosure under Rule 16(a)(1)(E)(i), the
19 evidence may be withheld under a law enforcement privilege. In *Roviaro*, the Supreme
20 Court held that the government had a privilege to withhold from disclosure the identities
21 of certain confidential informants. 353 U.S. at 59. Subsequent cases have expanded the
22 privilege to other investigative techniques, including software programs like Torrential
23 Downpour. See *Pirosko*, 787 F.3d at 366 (applying the privilege to the government's
24 Shareaza program); *United States v. Van Horn*, 789 F.2d 1492, 1508 (11th Cir. 1986)
25 (surveillance equipment); *United States v. Harley*, 682 F.2d 1018, 1020-21 (D.C. Cir.
26 1982) (surveillance locations).

27 The Supreme Court has declined to establish fixed rules for deciding whether the
28 government may withhold material information under a law enforcement privilege,

1 holding instead that trial courts must engage in balancing on a case-by-case basis:

2 We believe that no fixed rule with respect to disclosure is justifiable. The
3 problem is one that calls for balancing the public interest and protecting the
4 flow of information against the individual's right to prepare his defense.
5 Whether a proper balance renders non-disclosure erroneous must depend on
6 the particular circumstances of each case, taking into consideration the
7 crime charged, the possible defenses, the possible significance of the
8 informer's testimony, and other relevant factors.

9 *Roviaro*, 353 U.S. at 62. The trial court's balancing must afford due regard to the
10 government's interest in maintaining the secrecy of its investigative technique, but must
11 also fully protect the defendant's interest in a fair trial. When the two interests come
12 squarely into conflict, the defendant's right to a fair trial should prevail because the
13 government can always choose to protect its investigative technique by dropping the
14 prosecution and due process dictates that a citizen should never be convicted in an unfair
15 trial. *See United States v. Turi*, 143 F. Supp. 3d 916, 921 (D. Ariz. 2015).

16 Having considered the particular circumstances of this case and the factors to be
17 balanced under *Roviaro*, the Court finds that disclosure of an installable copy of
18 Torrential Downpour for testing by a third-party is not warranted. Child pornography is a
19 scourge, victimizing the most innocent for the basest of reasons. The government has a
20 legitimate interest in preserving its ability to investigate and prosecute distribution of this
21 material – distribution that creates the market and fuels the demand for creation of more
22 child pornography. Agent Daniels testified that the government's investigative efforts
23 would be severely hampered if a copy of Torrential Downpour got into the wrong hands.
24 Countermeasures could be developed that would thwart law enforcement's monitoring of
25 the BitTorrent network for suspected child pornography. Doc. 50 at 126:10-20. For this
26 reason, the government closely guards Torrential Downpour and limits the persons
27 granted access to it. He testified that the program must remain in law enforcement
28 custody at all times to avoid the risk of disclosure to unauthorized third-parties. *Id.*
at 126:23-128:15.

1 The Court concludes that this substantial government interest outweighs
2 Defendant Gonzales's need for an independent copy of Torrential Downpour. *See*
3 *Harney*, 2018 WL 1145957, at *11 (finding that the risk of inadvertent leaking by third
4 parties who would have access to the government's software outweighed the defendant's
5 need for such material). But given the substantial defense interest established by
6 Defendant Gonzalez, the Court concludes that his expert should be granted access to
7 Torrential Downpour for purposes of assisting in preparing the defense. The Court will
8 balance these interests by adopting the Rule 16 disclosure method authorized in *Crowe*:

9 [T]he defense expert [will be permitted] to examine the software at issue at
10 a designated law enforcement facility, at a mutually convenient date and
11 time, for as much time as is reasonably necessary for the expert to complete
12 her examination. No copies of the software shall be made. The software
13 shall not leave the custody of the law enforcement agency that controls it.
14 Any proprietary information regarding the software that is disclosed to the
15 defense expert shall not be reproduced, repeated or disseminated in any
16 manner. Violation of [this] order shall subject the defense expert and/or
17 defense counsel to potential sanctions by this Court.

18 2013 WL 12335320, at *8.⁴

19 The Court at this point will not require discovery of the Torrential Downpour
20 manuals. Defendant Gonzalez has not provided evidence or explained how the manuals
21 will aid in preparation of his defense. Defendant Gonzalez may raise this issue with the
22 Court if examination of the software by Loehrs suggests that the manuals would be
23 helpful to the defense, at which point the Court will hear from both parties before making
24 a decision.

25 **IT IS ORDERED:**

- 26 1. Defendant Gonzales's motion to compel discovery (Doc. 25, Case No. CR-
27 17-01311) is **granted in part** and **denied in part** as set forth in this order.
- 28 2. Defendant Ordonez's motion to compel discovery (Doc. 32, Case No. CR-

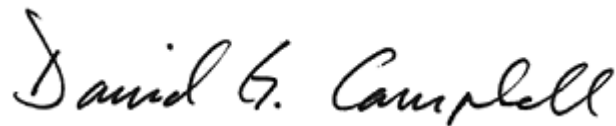
⁴ Agent Daniels made clear that such access would pose no security risk. Doc. 50 at 156:25-157:1-3.

1 18-00539) is **denied**.

2 Excludable delay pursuant to U.S.C. § 18:3161(h)(1)(D) is found to run from
3 6/28/2018 in Case No. CR17-01311 PHX DGC and 12/7/2018 in Case No. CR18-00539
4 PHX DGC.

5 Dated this 19th day of February, 2019.

6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



David G. Campbell
Senior United States District Judge

350 Fifth Avenue, 34th Floor
New York, NY 10118-3299
Tel: 212-290-4700
Fax: 212-736-1300; 917-591-3452



HRW.org

US PROGRAM

Nicole Austin-Hillery, *Executive Director*
Sara Darehshori, *Senior Counsel*
Dreisen Heath, *Senior Coordinator*
Elizabeth Kennedy, *Researcher*
Rachel Kent, *Press Officer*
Clara Long, *Senior Researcher*
Megan McLemore, *Senior Researcher*
Grace Meng, *Senior Researcher*
Alison Leal Parker, *Managing Director*
Laura Pitter, *Senior National Security Counsel*
Thomas Rachko, *Associate*
John Raphael, *Senior Researcher*
Brian Root, *Quantitative Analyst*
Sarah St. Vincent, *Researcher*
Jasmine L. Tyler, *Advocacy Director*

HUMAN RIGHTS WATCH

Kenneth Roth, *Executive Director*
Michele Alexander, *Deputy Executive Director, Development and Global Initiatives*
Iain Levine, *Deputy Executive Director, Program*
Chuck Lustig, *Deputy Executive Director, Operations*
Bruno Stagno Ugarte, *Deputy Executive Director, Advocacy*

Emma Daly, *Communications Director*
Peggy Hicks, *Global Advocacy Director*
Babatunde Olujobi, *Deputy Program Director*
Dinah Pokempner, *General Counsel*
Tom Porteous, *Deputy Program Director*
James Ross, *Legal & Policy Director*
Joe Saunders, *Deputy Program Director*
Frances Sinha, *Human Resources Director*

BOARD OF DIRECTORS

Hassan Elmasry, *Co-Chair*
Joel Motley, *Co-Chair*
Wendy Keys, *Vice-Chair*
Susan Manilow, *Vice-Chair*
Jean-Louis Servan-Schreiber, *Vice-Chair*
Sid Sheinberg, *Vice-Chair*
John J. Studzinski, *Vice-Chair*
Michael G. Fisch, *Treasurer*
Bruce Rabb, *Secretary*
Karen Ackman
Jorge Castañeda
Tony Elliott
Michael E. Gellert
Hina Jilani
Betsy Karel
Robert Kissane
David Lakhdir
Kimberly Marteau Emerson
Oki Matsumoto
Barry Meyer
Joan R. Platt
Amy Rao
Neil Rimer
Victoria Riskin
Graham Robeson
Shelley Rubin
Kevin P. Ryan
Ambassador Robin Sanders
Javier Solana
Siri Stolt-Nielsen
Darian W. Swig
Makoto Takano
John R. Taylor
Amy Towers
Peter Visser
Marie Warburg
Catherine Zennström

Matt Dummermuth
Principal Deputy Assistant Attorney General
US Department of Justice
810 Seventh St. NW
Washington, DC 20531

Cc: Caren Harp
Administrator, Office of Juvenile Justice and Delinquency Prevention
US Department of Justice

Michael Horowitz
Inspector General
US Department of Justice

Peter Winn
Acting Chief Privacy and Civil Liberties Officer
US Department of Justice

Re: Child Protection System software suite

February 1, 2019

Dear Mr. Dummermuth:

We write to ask questions and express concerns about Child Protection System (CPS), a software suite that federal and state law enforcement—including members of the Internet Crimes Against Children Task Force Program established by the Justice Department—use to investigate crimes related to the sharing of child sexual exploitation images.

Human Rights Watch has long promoted accountability for sexual abuse of children around the world, and recognizes that lawful and rights-protecting efforts to prosecute and punish those who commit such crimes are of utmost importance.¹ Our examination of CPS, however, raises several concerns that tie into broader problems in the US criminal justice system.

Specifically, we are concerned that:

¹ Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and pornography, UN Doc. A/RES/54/263 (March 16, 2001), art. 3(i)(c), <https://www.ohchr.org/en/professionalinterest/pages/opsccrc.aspx> (accessed October 29, 2018). Human Rights Watch has produced a substantial body of work investigating and advocating effective measures to curb sexual abuse of children. Some examples include Human Rights Watch, *Breaking the Silence: Child Sexual Abuse in India* (2013), <https://www.hrw.org/report/2013/02/07/breaking-silence/child-sexual-abuse-india>; Human Rights Watch, “End Child Marriage,” <https://www.hrw.org/EndChildMarriage>; and Saroop Ijaz, “Protect Pakistan’s Children from Sexual Abuse,” commentary, Human Rights Dispatch, August 14, 2018, <https://www.hrw.org/news/2018/08/14/protect-pakistans-children-sexual-abuse>.

- As has proven to be the case regarding other technical investigative methods US authorities have previously employed,² the CPS software may not have been subject to thorough independent testing of its accuracy and functioning. Since the system is designed to flag people as suspected of having committed crimes, both its error rates and its potential to exceed constitutional bounds have implications for rights. It is unclear what information the Justice Department has about CPS' potential for error (and on what basis), although prosecutors stated in one court filing that CPS mistakes are “practically nonexistent.”³
- CPS is provided by a non-profit organization that has repeatedly stated it offers the system exclusively to law enforcement, while prosecutors have argued that they cannot provide the software to criminal defense experts for testing because it is proprietary and not in the government's possession. We fear that the government may be shielding its methods from scrutiny by relying on its arrangements with the non-profit—one whose close relationship with police may, in fact, make it a government agent.
- The CPS software may be facilitating undisclosed police access, without legal process, to personal data about internet subscribers held by a datamining program that private credit reporting agency TransUnion owns. There appears to be a close relationship between the non-profit organization that offers CPS and this private credit reporting agency. If this is indeed occurring, such a practice would give rise to constitutional, federal, and human rights law and policy concerns.
- Among the potential issues arising from any such secret law enforcement access to personal data is that defendants and trial courts may not learn about, or be able to challenge, the breadth of information police obtain—and the potential for that information to facilitate decision-making based on implicit bias or other improper factors.
- Law enforcement may be concealing any such secret use of personal data by deliberately creating a new and different paper trail—a practice known as “parallel construction,” which our prior reporting suggests is a common and rights-harming problem in US prosecutions.⁴
- Potential errors by officers in identifying files as illicit—and registering them as such in a shared database—may harm legitimate free expression in a lasting manner. It is unclear whether any systematic review occurs to prevent this from happening.
- The available sources do not indicate what efforts the Justice Department or other law enforcement agencies make to ensure that any data incorrectly linking innocent people to the highly stigmatized offense of possessing child sexual abuse images is corrected or deleted.

This letter provides background and details regarding these concerns and seeks information from the Justice Department on or before February 18, 2019 about current policies and practices related to law enforcement uses of CPS.

² Recent examples include hair comparisons and bite-mark analysis. See, for example, President's Council of Advisors on Science and Technology, *Forensic Science in Criminal Courts: Ensuring the Scientific Validity of Feature-Comparison Methods* (2016), pp. 8-9, 13-14, 83-87, 118-122, <https://www.innocenceproject.org/wp-content/uploads/2017/03/PCAST-2017-update.pdf> (accessed October 30, 2018) (hereinafter “PCAST Report”).

³ *Infra* n. 22 and accompanying text.

⁴ Human Rights Watch, *Dark Side: Secret Origins of Evidence in US Criminal Cases*, January 2018, https://www.hrw.org/sites/default/files/report_pdf/us0118.pdf.

The discussion below is based on research we conducted between May 2016 and October 2018, including an examination of records from 20 federal prosecutions in which the government explicitly disclosed the use of CPS, as well as information appearing in a set of federal civil-rights lawsuits brought against local authorities in Mississippi in 2011 following the use of CPS there. (See Appendix for a list of these cases.) Although we do not address state cases here, media coverage and other sources suggest that prosecutions in state courts involving CPS use may be common.⁵

The CPS Software Suite

CPS is a set of software tools and databases designed to help law enforcement identify individuals who allegedly share child exploitation images on peer-to-peer networks, which enable internet users to connect to one another and trade files such as pictures, music, and videos. A US-based non-profit organization, Child Rescue Coalition (CRC), reports that it provides the software suite to law enforcement—including the Internet Crimes Against Children Task Force run by the Justice Department.⁶

It is our understanding that a CPS component called Peer Spectre monitors file-sharing traffic on peer-to-peer networks. Anyone on a peer-to-peer network can search for files by keyword, and we understand that Peer Spectre carries out continuous, automated keyword searching for suspicious file titles and identifies Internet Protocol (IP) addresses that are allegedly sharing those files. The results of these searches are logged in servers law enforcement can access.

We understand that a second component of CPS, Shareaza LE, then enables law enforcement to single out a particular IP address and attempts to download all the files it is sharing, a technique known as a “sole source download.” This gives police a means of investigating the tips CPS generates when it monitors the peer-to-peer network. Our information suggests that without Shareaza LE (which is not available to the public), peer-to-peer network users typically cannot carry out sole source downloads.

We understand that at these initial stages, suspected child exploitation images are identified using “hash values,” or unique digital identifiers roughly analogous to fingerprints, that can be calculated for many files using certain algorithms.

What is now CPS was apparently developed as part of a collaborative effort by law enforcement authorities and then was acquired by a data broker known as TLO, LLC, in

⁵ See, for example, Carey Codd, “Boca Raton-Based Child Rescue Coalition Works ‘To Find Those That Victimize Kids,’” *CBS4 News*, November 18, 2015, <https://miami.cbslocal.com/2015/11/18/boca-raton-based-child-rescue-coalition-works-to-find-those-that-victimize-kids/> (accessed December 12, 2018) (“The Broward State Attorney’s Office said they’ve prosecuted close to 150 cases based on information supplied by the Child Rescue Coalition”); *People v. Worrell*, 59 Misc. 3d 594 (N.Y.), March 2, 2018; *State v. Baric*, 2018 WI App. 63 (Wis. Ct. App.), September 18, 2018; *Frazier v. State*, 180 So. 3d 1067 (Fla. Dist. Ct. App.), November 20, 2015.

⁶ *United States v. McKinion*, no. 2:14-cr-00124 (C.D. Cal.), Declaration of William S. Wiltse (doc. 62-1), para. 2; Child Rescue Coalition Inc., Internal Revenue Service Form 990 (2017), p. 36; Department of Justice, “Office of Juvenile Justice and Delinquency Prevention’s Internet Crimes Against Children Task Forces Arrest More Than 1,000 Child Predators in Operation Broken Heart,” Press release, June 22, 2015, <https://www.justice.gov/opa/pr/office-juvenile-justice-and-delinquency-prevention-s-internet-crimes-against-children-task> (accessed October 30, 2018); Internet Crimes Against Children Task Force Program, <https://www.icactaskforce.org/> (accessed October 30, 2018).

2009.⁷ TLO was purchased by credit reporting agency TransUnion in 2013 after filing for bankruptcy and is now known as TLOxp.⁸ CRC, the non-profit organization that now offers CPS, was established in the wake of TLO's bankruptcy and continues to share a physical address with TLOxp.⁹

Reliability Testing Concerns: Accuracy and Reach

1. Accuracy

Concern has grown in recent years about how US courts regard technical investigative methods and whether those methods have been adequately tested to ensure their accuracy and consistency.¹⁰ Without rigorous testing, it is impossible to know objectively how often an investigative method produces false positives or false negatives, and what factors may affect those rates.¹¹

However, to date we have not found any public information on CPS having been tested by qualified independent experts or results of such testing.

Knowing the accuracy of investigative methods is important for human rights and constitutional reasons. Except in an emergency or other exceptional circumstance, US police may force people to submit to intrusive searches of their homes or electronic devices only if the authorities first obtain a warrant from a court based on a demonstration that they have probable cause to believe they will find evidence of a crime. To show that such probable cause exists, they may rely wholly or partly on results from an investigative tool such as CPS. If the tool has accuracy problems, its results may not provide a sufficiently sound basis for a court to include in the justification for issuing a warrant—and a warrant issued without probable cause is unconstitutional under the Fourth Amendment. In turn, under the “fruit of the poisonous tree” rule, trial courts will normally prohibit prosecutors from introducing any evidence that derives from an initial illegal search, such as one based on a warrant that lacked probable cause.¹²

⁷ See, for example, *United States v. Dang*, no. 6:16-cr-10027 (D. Kan.), Affidavit of William S. Wiltse (doc. 23-1), undated, filed September 26, 2016, para. 2; *United States v. Clements*, no. 1:15-cr-00275 (N.D. Ohio), Affidavit of William S. Wiltse (doc. 18-1), August 2, 2013, para. 2.

⁸ Jeff Ostrowski, “After founder’s death, Boca tech firm TLO files for Chapter 11,” *Palm Beach Post*, May 9, 2013, <https://www.mypalmbeachpost.com/business/after-founder-death-boca-tech-firm-tlo-files-for-chapter/34CcCzHza646WkCtWoWZuN/> (accessed October 30, 2018); TransUnion, “TransUnion Completes Acquisition of TLO,” <https://newsroom.transunion.com/transunion-completes-acquisition-of-tlo/> (accessed October 30, 2018); TransUnion and TLOxp, www.tloxp.com (accessed October 30, 2018).

⁹ CRC’s Form 990 tax filing for 2013 covers a period beginning December 11, 2013, suggesting that the organization was established on or around this date. Its address is listed on its 2017 Form 990; the same address is listed on TLOxp’s “Contact Us” page, <https://www.tlo.com/contact> (accessed October 31, 2018).

¹⁰ See, PCAST Report, *supra* n. 2, pp. 3-6; Rebecca Wexler, “Convicted by Code,” *Slate*, October 6, 2015, <https://slate.com/technology/2015/10/defendants-should-be-able-to-inspect-software-code-used-in-forensics.html> (accessed October 31, 2018); Jonathan Jones, “Forensic Tools: What’s Reliable and What’s Not-So-Scientific,” *Frontline*, April 17, 2012, <https://www.pbs.org/wgbh/frontline/article/forensic-tools-whats-reliable-and-whats-not-so-scientific/> (accessed October 30, 2018); Innocence Project, “Misapplication of Forensic Science,” undated, <https://www.innocenceproject.org/causes/misapplication-forensic-science/> (accessed October 30, 2018).

¹¹ See generally PCAST Report, *supra* n. 2, pp. 5-6.

¹² *Wong Sun v. United States*, 371 U.S. 471 (1963).

This means establishing a technique's error rates is critical both to protecting people from unconstitutional searches and to ensuring that in a criminal trial, the prosecution cannot unfairly benefit from illegal police activities.

HRW.org

Where software is concerned, the Justice Department's policy guidance states that such tools "used to support evidence discovery, extraction and examination, case examination and evaluation and method development shall be technically reviewed by qualified experts and validated prior to use."¹³ Materials the US Commerce Department's National Institute of Standards and Technology (NIST) has published help demonstrate that it is possible to develop a methodology for objectively testing how, and how reliably, software operates. For example, as part of a project concerning computer forensic tools, NIST has set out a testing process that includes, inter alia:

- The development of test cases, which are then posted online, along with other information, for "peer review by members of the computer forensics community and for public comment by other interested parties";
- The incorporation of feedback from the peer-review and public-comment processes;
- NIST's acquisition of the tool for testing;
- An examination of the available documentation;
- The selection of appropriate test cases;
- The development of a test strategy;
- The execution of the test; and
- The production and online posting of a test report.¹⁴

As noted above, despite the existence of such scientific methodologies and the Justice Department's policy, we have been unable to locate any evidence that CPS has been subjected to complete, independent, peer-reviewed testing. If such tests have been carried out, we request that you make the studies publicly available.¹⁵

When defendants have made motions seeking to arrange for expert testing of the software, federal prosecutors have sometimes sought to avoid producing CPS' source code for testing on the grounds that it is protected from disclosure by law enforcement privilege,¹⁶ that the code is proprietary and not in the government's possession¹⁷—or both.¹⁸ We have identified only one case—*United States v. Ocasio*—in which prosecutors ultimately produced the CPS

¹³ U.S. Department of Justice, "Scientific Research and Integrity Policy," undated, <https://www.justice.gov/olp/forensic-science> (accessed December 6, 2018), p. 6.

¹⁴ National Institute of Standards and Technology, "Methodology Overview," February 22, 2018, <https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-general-o> (accessed October 30, 2018).

¹⁵ CRC's president William Wiltse testified during a 2013 hearing concerning a defense motion to suppress in *United States v. Thomas*, a Vermont federal case, that some aspects of the CPS suite were tested internally to a certain degree when CPS was first developed, but that the suite had not been tested more recently or subjected to thorough, independent testing using a standardized process. *United States v. Thomas*, no. 5:12-cr-00037 (D. Vt.), "Transcript: Motion to Suppress & Request for a Franks Hearing," (doc. 99), April 17, 2013, pp. 102-110.

¹⁶ See, for example, *United States v. Dang*, *supra* n. 7, Response to Defendant's Motion to Compel Production (doc. 23), September 26, 2016, p. 12; *United States v. Hartman*, no. 8:15-cr-00063 (C.D. Cal.), Opposition to Defendant's Motion to Compel Discovery (doc. 37), September 24, 2015, p. 4.

¹⁷ See, for example, *United States v. Neale*, no. 5:12-cr-00044 (D. Vt.), Response to Defendant's Motion to Compel Discovery (doc. 44), December 7, 2012, pp. 8-10; *United States v. Crowe*, no. 1:11-cr-01690 (D.N.M.), Response to Defendant's Motion to Compel and Motion to Inspect (doc. 58), June 1, 2012, pp. 11-15.

¹⁸ *Ibid.*; *United States v. Dang*, *supra* n. 7, Response to Defendant's Motion to Compel Production (doc. 23), September 26, 2016, pp. 12, 23-24.

source code to a defendant, and a statement submitted in a later case suggests that *Ocasio* was resolved through a plea agreement before any expert testing took place.¹⁹

HRW.org

By contrast, in a 2015 decision in *United States v. Naylor*, a West Virginia federal court simply accepted an officer's assertion that in his personal experience, the tool had never erred and was (in the court's words) "100% reliable."²⁰ The court therefore concluded that "[t]he CPS software appears to be a reliable investigative tool for law enforcement in these types of cases" and rejected the defendant's motion to suppress evidence found through the software.²¹ In at least one case, the government itself has asserted in a motion that "[e]rror is practically nonexistent in the Shareaza LE and CPS systems" without citing any sources for this claim.²²

We fear this situation—in which prosecutors resist defense testing of CPS but are willing to make, or apparently allow witnesses to make, assertions about the software's accuracy—may interfere with the judiciary's ability to assess the tool's potential for malfunction, and thus jeopardize fair-trial rights.

Regarding assertions that CPS' source code is proprietary or otherwise not in the government's possession, we note that CRC has consistently described itself as heavily enmeshed with and dedicated to furthering the operations of law enforcement. In its tax filings, the organization has stated that it "offers space at its operational location to law enforcement agencies in order to easily access the tracking system."²³ Affidavits by the group's president, William Wiltse, have described access to CPS as "made available to specifically trained and licensed law enforcement officers and ... *restricted to only those law enforcement officers in the performance of law enforcement activity*" (emphasis added).²⁴ Testimony by Wiltse in 2013 concerning CPS-enabled investigations (prior to the establishment of CRC) described a "restricted area" on TLO's property: "The only people allowed into this area are sworn law enforcement officers. Even our boss, our CEO, cannot get into this area without being escorted," Wiltse told the court.²⁵ Wiltse himself is a reserve deputy sheriff for Florida's Palm Beach County, according to his affidavits and CRC's website.²⁶

¹⁹ For the decision granting the defendant's motion to compel production of the CPS source code in *United States v. Ocasio*, no. 3:11-cr-02728 (W.D. Tex.), see 2013 U.S. Dist. Lexis 79313 (2013 WL 2458617), June 6, 2013. For a discussion concerning how *Ocasio* was resolved, see *United States v. Shia*, no. 3:15-cr-00257 (N.D. Cal.), Affidavit of Tami Loehrs Re Ocasio Case (doc. 27), November 19, 2015.

²⁰ *United States v. Naylor*, 99 F. Supp. 3d 638, 643 (S.D.W. Va., 2015).

²¹ *Ibid.*

²² *United States v. Pirosko*, no. 5:12-cr-00327 (N.D. Ohio), Response in Opposition to Defendant's Motion to Compel (doc. 32), August 2, 2013, pp. 7-8. To the best of our knowledge, the case the government mentioned in the second part of the sentence involved a different software program.

²³ See, for example, Form 990 (2017), *supra* n. 9, p. 36.

²⁴ *United States v. Dunning*, no. 7:15-cr-00004 (E.D. Ky.), August 26, 2015, Affidavit of William S. Wiltse (doc. 30-1), September 14, 2015, para. 13; *United States v. Crowe*, *supra* n. 17, Affidavit of William S. Wiltse (doc. 58-1), June 1, 2012, para. 3; *United States v. Clements*, *supra* n. 7, Affidavit of William S. Wiltse (doc. 18-1), August 2, 2013, para. 3.

²⁵ *United States v. Thomas*, *supra* n. 15, Transcript, pp. 131-32.

²⁶ *United States v. Dunning*, *supra* n. 24, Affidavit of William S. Wiltse, para. 1; Child Rescue Coalition, "Our Team," <https://childrescuecoalition.org/our-team/> (accessed October 31, 2018).

We therefore regard government arguments that prosecutors cannot produce the CPS source code for testing as both inappropriate and jeopardizing fair-trial rights, insofar as access to the source code is necessary for scientifically sound testing.²⁷

2. Reach

Accuracy is not the only aspect of CPS that is susceptible to testing and should be subject to scientifically sound validation prior to law enforcement use. The software suite's reach also has potential constitutional consequences.

Federal courts have found that police do not need a search warrant to monitor peer-to-peer network activities that take place in public,²⁸ and CRC's president has maintained that the CPS software only locates information that peer-to-peer network users have publicly shared.²⁹ If this description of CPS is correct, then under current US constitutional law, police may use or rely on the software without obtaining a warrant first.

However, defendants in several federal cases have offered evidence that files (or traces of files) officers have identified using CPS may have been stored in areas of their devices that were not publicly shared, raising Fourth Amendment concerns.³⁰ We acknowledge that the strength of this evidence is open to debate and that federal prosecutors have challenged the credibility of the forensic expert who produced the relevant reports. However, nowhere in the records we reviewed does the government actually set out evidence refuting the claims that CPS can reach beyond publicly shared folders, let alone persuasively show that the software cannot do so or is not being so used.³¹

This, too, is a matter that rigorous independent testing can and should resolve.

Free Speech and Related Concerns

To function accurately, CPS depends not only on the correct identification of IP addresses and the hash values of shared files, but on police officers correctly designating files as containing illegal child exploitation images. The potential for mistakes in this respect prompts concerns about the resulting impact on legitimate free expression, particularly if the Justice Department does not ensure that these designations are regularly reviewed.

²⁷ See, also, Rebecca Wexler, "Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System," *Stanford Law Review*, vol. 70 (May 2018), pp. 1364-65, 1429, <https://review.law.stanford.edu/wp-content/uploads/sites/3/2018/06/70-Stan.-L.-Rev.-1343.pdf> (accessed October 31, 2018) (specifically addressing the CPS case *Ocasio* and concluding that "extending the [trade secret] privilege wholesale from civil to criminal proceedings is both harmful and unnecessary").

²⁸ See, for example, *United States v. Thomas*, 2013 WL 6000484 (D. Vt. 2013), 47-51 (aff'd 2d Cir., 788 F. 3d 345, 351 (2015)); *United States v. Baalerud*, 2015 WL 1349821 (W.D.N.C. 2015), pp. 23-26; *United States v. Dodson*, 960 F. Supp. 2d p. 689, pp. 695-696 (W.D. Tex. 2013).

²⁹ See, for example, *United States v. Clements*, *supra* n. 7, Affidavit of William S. Wiltse (doc. 18-1), August 2, 2013, para. 8; *United States v. Crowe*, *supra* n. 25, Affidavit of William S. Wiltse (doc. 58-1), May 31, 2012, para. 6.

³⁰ *United States v. Clements*, *supra* n. 7, Affidavit of Tami Loehrs (doc. 17-2), November 19, 2015, para. 10; *United States v. Crowe*, *supra* n. 25, Affidavit of Tami Loehrs (doc. 48-1), April 26, 2012, paras. 11, 14-16; *United States v. Dang*, *supra* n. 7, Affidavit of Tami Loehrs (doc. 19-1), August 9, 2016, para. 11; *United States v. Hartman*, *supra* n. 24, Affidavit of Tami Loehrs (doc. 50-1), October 8, 2015, paras. 14-16.

³¹ See, for example, *United States v. Hartman*, *supra* n. 16, Order Re Pretrial Motions (doc. 87), November 24, 2015, pp. 22-23 (noting that "the Government has not refuted the defense expert's analysis that suggests the files at issue here were not designated as shareable," although it had had "ample opportunity to do so").

An affidavit by Wiltse in an Ohio federal prosecution, *United States v. Clements*, and his 2013 testimony in *Thomas* indicate that officers using CPS may designate newly discovered files as “Child Notable” based on their own opinions and proceed to register hash values for those files in one or more of the system’s networked databases.³² Wiltse’s testimony in *Thomas* further indicates that CPS’ reliance on these officer-made designations is extensive.³³ However, the records we have examined do not disclose any systematic safeguards for ensuring that these designations are accurate. This raises concerns that people’s right to access and receive information—part of the right to free expression—could be at risk if officers mischaracterize files, or generate records when someone possesses lawful files (such as legal adult pornography).

Additionally, we understand that the element of the software suite called Shareaza LE gives officers the technical ability to view the hash values of, and download, *any* file an IP address is sharing on a peer-to-peer network—regardless of whether those files are believed to be illicit.³⁴ The Justice Department should explain whether it takes steps to ensure officers are not monitoring legitimate free expression in a manner that would be inconsistent with rights laws or policies.

Personal Data and Discrimination Concerns

Through our research, we have become aware of potential law enforcement access to personal information when using CPS. This potential for access could undermine privacy and consumer protections found in federal law, reduce defendants’ ability to learn about and challenge any abusive practices, and facilitate improper decision-making.

An undated user agreement for the CPS software submitted as evidence in a 2015 California criminal prosecution, *United States v. Hartman*, suggests that CPS users have—or have had—free access to “Unconfirmed Subscriber Data provided by TLO.”³⁵ “Subscriber” is apparently a reference to people who subscribe to internet services and therefore are associated with an IP address, while “TLO” is a reference to the datamining operation now known as TLOxp.

³² *United States v. Clements*, *supra* n. 7, Affidavit of William S. Wiltse, para. 9 (“The term ‘Child Notable’ is an *investigator assigned* category for certain file hashes within the Child Protection System.... During training investigators are provided software, which generates hash values for recently located child exploitation files and submits those hash values to CPS databases *with a category selected by the investigator*” (emphasis added)); *United States v. Thomas*, *supra* n. 23, Transcript, pp. 56-57 (“[L]aw enforcement has been aware and continues to become aware of new pieces of child pornography that are being made available on these [peer-to-peer] file sharing networks.... What law enforcement is trained to do is submit the hash values, so we actually give them tools that calculate the hash value for these files, but then law enforcement can then electronically submit those hash values to us, along with a category that the officer is trained to use as far as what is it that this file is categorized as based on your training, and then we then can leverage that hash value or the knowledge of that hash value in programs such as Peer Spectre. So what I mean by that is Peer Spectre is aware of hundreds of thousands of pieces of what *investigators describe as* child notable, which I guess for all intents and purposes is child pornography” (emphasis added)).”

³³ *United States v. Thomas*, *supra* n. 23, Transcript, pp. 56-57 (“Peer Spectre is aware of *hundreds of thousands* of pieces of what investigators describe as child notable [files]” (emphasis added)).

³⁴ See, for example, *United States v. Clements*, *supra* n. 7, doc. 22-6 (filed March 16, 2016); *United States v. Naylor*, *supra* n. 24, no. 2:14-cr-00194 (S.D.W. Va.), doc. 19-1 (filed January 6, 2015), p. 17 of file. These documents are CPS screenshots indicating that officers using the software suite can see that an individual is sharing files that are “Not Categorized,” “Adult Erotic,” or of “No Known Relevance,” in addition to known or suspected “Child Notable” files.

³⁵ *United States v. Hartman*, *supra* n. 16, “The Child Protection System – Acceptable Use Requirements” (doc. 102-2), undated, filed January 8, 2016, p. 2.

This “Unconfirmed Subscriber Data” might include marketing data about individuals—such as names, telephone numbers, addresses, and dates of birth—that corporate sources have linked to their IP addresses and email accounts. It is our understanding that officers using CPS have been told that no logs will be kept of any search they may perform of this corporate data.

Can you confirm what “Unconfirmed Subscriber Data” includes, from whence it is derived, and the means by which TLOxp could identify IP addresses with specific individuals? We would also like to understand why no records would be kept of law enforcement queries of this data, and whether that is, in fact, the practice.

TLOxp’s website indicates that the information the datamining system possesses about an individual may include addresses and phone numbers;³⁶ records from automated license plate readers,³⁷ which can reveal where a car has traveled; information from drivers’ licenses;³⁸ Social Security numbers;³⁹ employment records;⁴⁰ social media profiles, including photographs;⁴¹ criminal records;⁴² and connections to other people.⁴³ Please provide your understanding of what types of data CPS users, via TLOxp, may be able to view.

Under the Electronic Communications Privacy Act (ECPA), electronic communications service providers normally may only disclose information identifying the subscriber linked to an IP address in response to a subpoena or other legal process—thus leaving a paper trail defendants can obtain and scrutinize.⁴⁴ ECPA also limits the types of subscriber information the provider is obligated to disclose when responding to such a subpoena: primarily name, address, dates and durations of online sessions, and payment information.⁴⁵ While ECPA is outdated in many respects and subpoena powers are themselves susceptible to misuse,⁴⁶ these provisions nevertheless impose a significant privacy protection and create transparency about both the law enforcement demand and the data disclosed in response to it.

Our understanding is that TLOxp and CRC are not communications service providers and that ECPA therefore does not technically apply to their disclosure of data concerning people linked to IP addresses. However, we are concerned that the use of data from a data broker to identify subscribers without a subpoena or other legal process would subvert the protections Congress intended to establish in the law. Can you provide the details of what types of personal data law enforcement may be able to obtain when using CPS—and whether

³⁶ TransUnion, “TLOxp for Law Enforcement,” <https://www.tlo.com/law-enforcement> (accessed November 5, 2018).

³⁷ TransUnion, “TLOxp Vehicle Sightings,” <https://www.tlo.com/vehicle-sightings> (accessed November 5, 2018).

³⁸ TransUnion, “TransUnion’s TLOxp for Law Enforcement,” 2017, <https://www.tlo.com/resources/tlo/doc/industry/resources/industry-law-enforcement-as.pdf> (accessed December 17, 2018), p. 2.

³⁹ “TLO for Law Enforcement,” *supra* n. 36.

⁴⁰ *Ibid.*

⁴¹ TransUnion, “TLOxp Social Media Search,” <https://www.tlo.com/social-media> (accessed November 5, 2018); “About TLOxp,” *supra* n. 3.

⁴² TransUnion, “TransUnion’s TLOxp for Law Enforcement,” *supra* n. 38, p. 1.

⁴³ TransUnion, “TLOxp Relationship Report,” <https://www.tlo.com/relationship> (accessed November 5, 2018).

⁴⁴ 18 U.S.C. §§ 2702-03.

⁴⁵ 18 U.S.C. § 2703(c).

⁴⁶ See Human Rights Watch, *Dark Side*, *supra* n. 4, pp. 28-29.

that data may go beyond what a communications service provider would normally disclose under ECPA?

As noted above, TLOxp's technical means of linking individuals to IP addresses also remain unclear. These methods could raise further constitutional or other legal questions when the data is used by law enforcement, rendering the disclosure of information about them desirable to ensure respect for rights. We would appreciate any information you may have as to these technical means, and whether and to what sort of technical or legal review they may have been subjected.

Our understanding of the typical progression of a CPS-enabled investigation is that the software's broad monitoring of peer-to-peer networks results in a database of IP addresses that are suspected of offering illicit files, and that officers can then use a different component of CPS in an attempt to create a complete log of all the files a specific IP address is sharing. At this stage, under ECPA, officers would have the power to issue a subpoena directly to the internet service provider and thereby obtain the name and address of the relevant internet subscriber. Our review of relevant cases suggests that such subpoenas are typically disclosed to defendants, who are then able to review these records. Can you explain why officers may choose to not use the ECPA, which provides a record to courts and defendants, to obtain a defendant's name and address, opting instead to use TLOxp for this purpose?

We further note that CRC's website claims the non-profit offers "[a]nalytics targeting the offenders at greatest risk of presently abusing children."⁴⁷ The Justice Department should disclose whether police are receiving the results of such "[a]nalytics," and if so, what data the non-profit uses—or enables officers to use—when making these calculations.

Fundamental Rights Concerns: Parallel Construction

While "Unconfirmed Subscriber Data" from what is now TLOxp appears to be (or have been) available to CPS users, only one case we examined includes a record openly referring to this practice. It is possible that this absence of disclosures is due to officers' decisions not to view or use this data even though CRC has offered it. However, we are concerned that law enforcement may be gaining access to this personal data from or through CRC, and then deliberately concealing how officers obtained the information by re-obtaining it in other ways for use in court—a practice known as parallel construction. In our 2018 report *Dark Side: Secret Origins of Evidence in US Criminal Cases*, we documented evidence suggesting law enforcement has at times used parallel construction to conceal the original sources of leads in some criminal cases.⁴⁸

Parallel construction can prevent courts from reaching important or novel questions about constitutional rights, and defendants from arguing that judges should exclude unconstitutionally obtained evidence under the "fruit of the poisonous tree" rule. The

⁴⁷ Child Rescue Coalition, "The Solution," <https://childrescuecoalition.org/the-solution/> (accessed December 20, 2018).

⁴⁸ Human Rights Watch, *Dark Side*, *supra* n. 4, p. 1.

practice can also prevent defendants from learning that the government obtained exculpatory evidence during its investigation.⁴⁹

As noted above, if police were attempting to obtain the identity of a subscriber associated with an IP address from an internet or telephone service provider, they would need to issue a subpoena.⁵⁰ However, the CPS user agreement disclosed in 2016 instructs, “Do not use this [data from TLO] for probable cause. It must be confirmed through other investigative means that are acceptable with your agency and prosecuting attorney.”⁵¹ This reference to using “other investigative means” to “confirm[]” personal data previously obtained by another method prompts concerns that officers may employ parallel construction to avoid revealing that their initial leads came from personal data obtained from TLOxp. Can you comment on whether this has been a practice, or whether there are measures to prevent such practices in place?

The potential use of subpoenas as a means of “parallel construction” in a different context is currently the subject of an investigation by the Justice Department’s Office of the Inspector General.⁵² We encourage the Inspector General, to whom we will send a copy of this letter, to expand its investigation to determine whether such use of subpoenas is occurring in this context as well, and hope you will support such an effort.

In a California federal prosecution, *United States v. McKinion*, a Homeland Security Investigations special agent in Los Angeles used CPS to identify two different IP addresses as allegedly possessing unlawful child sexual abuse images in May 2012.⁵³ The agent’s search warrant application stated that “throughout ... April 2012,” the agent had “conducted records checks” for McKinion, including searches of address records and employment history.⁵⁴ The agent issued either a single subpoena or two subpoenas on the same date to the relevant internet service provider regarding the two IP addresses in May 2012.⁵⁵

In his affidavit, the agent did not explain what databases he used for his “records checks,” why he had conducted such checks concerning McKinion in April 2012 if the suspected illicit activities were only detected beginning in May 2012, or whether or how he linked both IP addresses to McKinion prior to issuing the subpoena(s)—especially when one of the IP addresses was shared with seven other people.⁵⁶ Likewise, prosecutors did not explain precisely how the two different IP addresses had been linked to the defendant, instead stating simply that the special agent “determined that Suspect IP 1 belonged to defendant and that defendant used Suspect IP 2.”⁵⁷

⁴⁹ *Ibid.* at pp. 3, 57, 59.

⁵⁰ 18 U.S.C. § 2703(c)(2).

⁵¹ *United States v. Hartman*, doc. 102-2, *supra* n. 16, p. 2.

⁵² Office of the Inspector General, U.S. Department of Justice, “Ongoing Work,” <https://oig.justice.gov/ongoing/all.htm> (accessed November 5, 2018).

⁵³ *United States v. McKinion*, *supra* n. 6, Affidavit in Support of Search Warrant (doc. 49-2), July 23, 2012, paras. 30-32. **Please be aware that these paragraphs contain graphic and disturbing descriptions of child sexual abuse images.**

⁵⁴ *Ibid.* at paras. 35-38.

⁵⁵ *Ibid.* at paras. 33-34.

⁵⁶ *Ibid.* at para. 34; see also *United States v. McKinion*, *supra* n. 6, Motion to Suppress Evidence Derived from Search Warrant (doc. 47), May 15, 2017, pp. 15-16.

⁵⁷ *United States v. McKinion*, *supra* n. 6, Opposition to Defendant’s Motion to Suppress Evidence (doc. 49), May 22, 2017, p. 6. The structure of the discussion in this paragraph implies without stating that the special agent made this determination before issuing a subpoena to internet service provider Catalina Computers.

We are concerned that parallel construction may have been employed in this case to avoid the disclosure of investigative activities prior to April 2012 and/or the use of databases that may have linked the IP addresses to individuals' names, and invite the Justice Department to comment on this.

HRW.org

Correcting Mistakes

Human Rights Watch is also concerned about whether CRC or law enforcement delete or correct data incorrectly linking innocent people to the possession of child sexual exploitation materials and, if so, how this is done.

Ensuring the deletion or correction of inaccurate data is essential to respecting rights and dignity. This is especially true when individuals may be wrongly suspected of illicit file-sharing because someone else used their internet services or devices for illegal activities without their knowledge. Police investigations of alleged downloads of child abuse images involving shared wi-fi networks and computers have previously led to questioning and searches impacting innocent people.⁵⁸ One such investigation in Jackson, Mississippi in 2011 that involved CPS led to a civil-rights lawsuit against local police.⁵⁹

Wiltse, CRC's president, also acknowledged in a 2017 declaration in *McKinion* that if a malicious hacker gained access to the nonprofit's tools, he or she could "implicate an innocent person's IP address as participating in the collection, manufacture or distribution of child exploitation files."⁶⁰ Such a possibility, no matter how seemingly remote, further supports the need for safeguards at all stages in the collection, storage, and sharing of personal data related to such law enforcement activities.

Questions for the Justice Department

In light of the foregoing discussion of concerns, we request that the Justice Department provide answers to the following questions:

Testing

- Has the Justice Department conducted or commissioned thorough independent third-party testing of CPS? If so, what methodology was used and what were the results? If not, does the use of CPS comply with the Department's policy regarding the validation of software tools?

⁵⁸ See, for example, *Tuskan v. Jackson County*, *infra* n. 59; Sam Stanton, "He wanted to download child porn, so he hacked his neighbor's wifi," *Sacramento Bee*, August 1, 2017, <https://www.sacbee.com/news/local/crime/article164803532.html> (accessed December 7, 2018); Anthony Bellano, "Man Was Pirating Neighbor's Wi-Fi To Download Child Pornography: Prosecutor," *Patch*, September 12, 2016, <https://patch.com/new-jersey/gloucestertownship/clementon-man-was-pirating-neighbors-wi-fi-download-child-pornography> (accessed December 7, 2018); Brett Cihon, "Prosecutor: Man sets up neighbor's Wi-Fi, secretly uses it to download child porn," *Q13 FOX*, April 9, 2014, <https://q13fox.com/2014/04/09/prosecutor-man-sets-up-neighbors-wi-fi-secretly-uses-it-to-download-child-porn/> (accessed December 7, 2018); Debra Cassens Weiss, "Prosecutor's Apology for Home Raid Highlights the Dangers of Unprotected WiFi," *ABA Journal*, March 18, 2011, http://www.abajournal.com/news/article/prosecutors_apology_for_home_raid_highlights_the_dangers_of_unprotected_wif/ (accessed December 7, 2018).

⁵⁹ *Tuskan v. Jackson County*, 2016 U.S. Dist. Lexis 182700 (S.D. Miss., 2016); for an investigative document showing the use of CPS, see case document 60-9 (case no. 1:13-cv-00356).

⁶⁰ *United States v. McKinion*, *supra* n. 6, Declaration of William S. Wiltse (doc. 62-1), October 27, 2017, paras. 15-16.

- Does the Justice Department have policies or practices that relate to the involvement of private or nongovernmental entities in conducting or facilitating law enforcement operations, and if so, what are they?
- What are the Justice Department’s policies regarding the level of technical expertise and access to software source code an officer should possess before prosecutors call him or her to testify about the software’s functioning and results? Before an officer or agent may attest to the software’s results in a search warrant application?
- Does the Justice Department require federal agents to receive training before using CPS? If so, what is the content of this training?

Free Speech

- Has the Justice Department assessed what proportion of files designated as “Child Notable” in CPS or relevant databases constitute unlawful child sexual exploitation images under federal or state law?
- Has the Justice Department analyzed the First Amendment implications of law enforcement use of CPS?

Personal Data and Discrimination Concerns

- Does the Justice Department permit agents to view subscriber data offered by CRC or TLOxp?
- Does the Justice Department believe logs should be kept of law enforcement access to such data? Are such logs kept?
- If agents are permitted to view the data, what types of information are included? What information links individuals’ identities to IP addresses, and from what source does that information come?
- Has the Justice Department analyzed whether the protections of the FCRA apply, or should be applied as a matter of policy, to data from TLOxp or CRC? If so, what were the conclusions of this analysis and in what document(s) do they appear?

Parallel Construction

- What are the Justice Department’s positions concerning the disclosure of an agent’s viewing or use of subscriber data from CRC or TLOxp to courts and defendants? Does the Justice Department require such disclosure if law enforcement subsequently obtains the information in question from other sources?
- Is the Justice Department aware of any use of parallel construction to conceal aspects of investigations involving CPS?
- Does the Justice Department have in place any rule, guidance or measure to prevent or disclose the use of parallel construction in obtaining evidence?

Correcting Mistakes

- What are the Justice Department’s policies and practices regarding the identification and treatment of investigative data incorrectly linking an individual, IP address, or device to the possession or sharing of illicit files? What are its policies and practices

regarding whether and how people who may have been wrongly linked to such activities should be notified?

- What are the Justice Department’s policies and practices regarding how electronic evidence linking an individual to a suspected offense should be stored and secured? Has the Justice Department determined that CRC is in compliance with these policies, if any?

* * *

We are aware that CPS is not the only software that may be capable of monitoring file-sharing networks for allegedly illegal images, and many of our concerns about this software suite may also apply to other systems. We believe answers to the foregoing questions will assist Congress, the courts, and the public in understanding the Justice Department’s treatment of both CPS and other comparable systems, and the broader issues raised by the use of such systems.

We thank you for your attention to this matter and await your response on or before February 18, 2019.

Sincerely,



Sarah St.Vincent
Researcher/Advocate on National Security, Surveillance, and Domestic Law Enforcement
Human Rights Watch

Encl.

Appendix: List of federal cases examined by Human Rights Watch

**Appendix:
List of Federal Cases Examined by Human Rights Watch**

Federal prosecutions

United States v. Baalerud (W.D.N.C., 3:14-cr-00188)

United States v. Brooks (M.D. Fla., 3:13-cr-00058)

United States v. Clements (N.D. Ohio, 1:15-cr-00275)

United States v. Crowe (D.N.M., 1:11-cr-01690)

United States v. Dang (D. Kan., 6:16-cr-10027)

United States v. Dennis (N.D. Ga., 3:13-cr-00010)

United States v. Dodson (W.D. Tex., 4:13-cr-00014)

United States v. Dunning (E.D. Ky., 7:15-cr-00004)

United States v. Hart (W.D. Wash., 3:14-cr-05507)

United States v. Hartman (C.D. Cal., 8:15-cr-00063)

United States v. Juhic (S.D. Iowa, 4:16-cr-00162)

United States v. Leikert (D. Vt., 5:12-cr-00097)

United States v. McKinion (C.D. Cal., 2:14-cr-00124)

United States v. Naylor (S.D.W. Va., 2:14-cr-00194)

United States v. Neale (D. Vt., 5:12-cr-00044)

United States v. Ocasio (W.D. Tex., 3:11-cr-02728)

United States v. Pirosko (N.D. Ohio, 5:12-cr-00327)

United States v. Price (S.D. Fl., 0:12-cr-60016)

United States v. Shia (N.D. Cal., 3:15-cr-00257)

United States v. Thomas (D. Vt., 5:12-cr-00037)

Federal civil actions

Brushaber v. Jackson County, Mississippi et al. (S.D. Miss., 1:13-cv-00453)

Pardue v. Jackson County, Mississippi et al. (S.D. Miss., 1:14-cv-00290)

Peairs v. Jackson County, Mississippi et al. (S.D. Miss., 1:13-cv-00402)

Tuskan v. Jackson County, Mississippi et al. (S.D. Miss., 1:13-cv-00356)

The Child Protection System

Child Protection System, or CPS, is a suite of programs centered on a web-based interface that provides access to investigative data gathered by automated tools and law enforcement searches. Traditionally IP based investigations have not allowed law enforcement to associate IP information with user data. By using CPS, investigators now have the option to correlate various data sources with IP addresses and screen names involved in criminal activity. All reports follow a standard convention in an easy to read format, which allows the investigator the ability to associate information.

The Child Protection System (CPS) allows trained investigators to identify offenders using peer-to-peer networks to distribute child pornography. Information is gathered by various automated tools and manual searches by law enforcement and accessed through CPS. This data can be used by investigators to gather, profile and track information tied to an Internet Protocol address (IP address) of the offender.

The Child Protection Systems provides a number of benefits to investigators. CPS future enhancements continue; here are a few of the current features:

- Investigators can quickly view activity of a specific IP address including other investigator interests in the IP address.
- Search by usernames (for example, superdad38@yahoo.com).
- File hashing - Files hash values in various formats.
- GUID (Globally Unique Identifier) histories reveal if other investigators have previously identified, shared interests and location information about that GUID. A GUID also may allow offender tracking across multiple IPs.
- Address searches reveal if other investigators have shared interest in an address (important for deconfliction). Latitude and longitude can be used to map addresses.
- Phone number searches reveal if other investigators have shared interest in an address (important for deconfliction).
- Service Providers provide legal contact information.

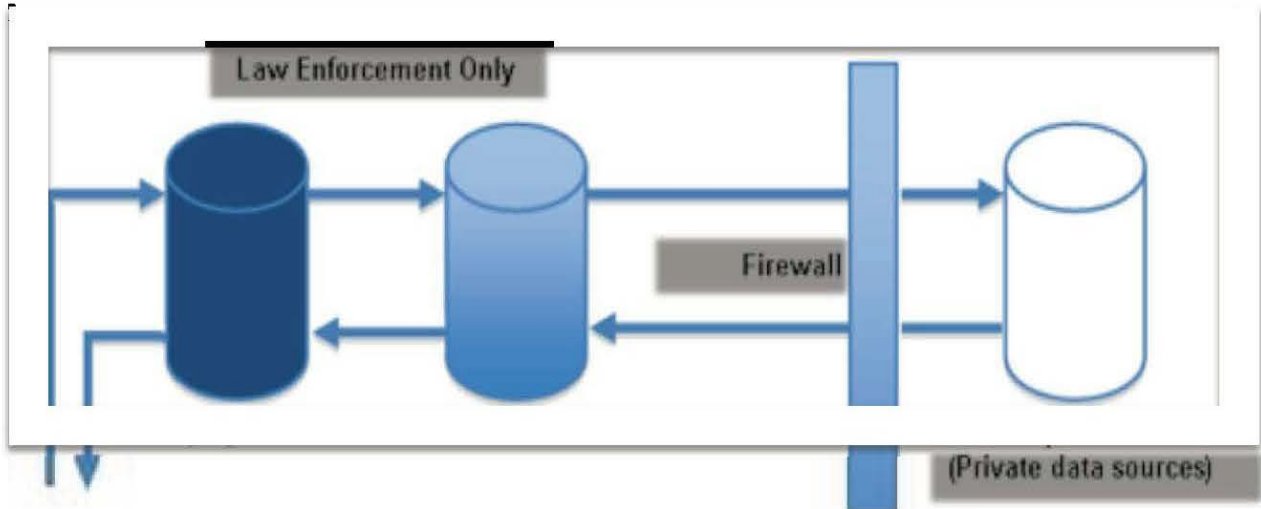
CPS is the web interface allowing the investigator to query the database, provide deconfliction, and investigative job creation. Licensed investigators, using their Gridcop username and password, may access the site at <https://cps.gridcop.com>.

CPS Data Sources

In CPS, the investigator has access to different data sources. Traditionally, all data generated by law enforcement personnel, or tools written by law enforcement, have been stored on servers located at the Wyoming Division of Criminal Investigation in Cheyenne, WY. In May of 2009, when the Wyoming servers failed, a second set of servers, purchased by TLO in Florida, and donated to the State Attorney for the Fifteenth Judicial Circuit, came online to provide replication, and are synchronized, allowing for redundancy, should one fail. Wyoming Toolkit users and automated tools such as Peer Spector contribute data to these servers.

With the assistance of TLO, an additional set of law enforcement only servers was added in Florida to store the increased volume of data generated by the software tools written by corporate

employees. These tools, including various crawlers and Peer Spectre2 (covered in other manuals), have the ability to capture more complete data on P2P targets, including GUIDs, firewall information, and push proxies (intermediary for requests).



The investigator also has the option of including private data sources in reports generated through CPS. TLO has allowed law enforcement access to data collected on Internet users from a variety of sources. This data includes marketing data that has been linked to IP addresses and email accounts from corporate sources. This data is considered unverified subscriber information and should never be considered a replacement for the subpoena or legal process, but is provided as intelligence information only. No logs are kept of any law enforcement query of corporate data, and TLO has no access to any law enforcement server.

When a law enforcement officer initiates a query, it is first directed to one of the two Fairplay servers where deconfliction is handled; the request is then sent to the TLO law enforcement server where the results are compiled. If the investigator chooses, the query is then sent to the corporate database for any unconfirmed subscriber information. The transaction with the corporate server is one-way and nothing is logged on the corporate server.

CPS Main Page

The home screen of CPS is divided into two main sections:

Manual searches. These text boxes allow searches for individual types of data, such as usernames, IP addresses, file hashes, GUIDs and other information.

Preformatted reports. These links provide access to the most commonly used queries. The user may drill down further in each report, depending on the level of information needed.

TLO Child Protection System - Data Lookup Currently logged in as User, Test. [Profile](#) | [Log Out](#)

Username(s):

IP Address(es):

File Hash(es):

GUID(s):

Service Providers:

Investigator:

Physical Address:

City:

State/Province:

Country:

Phone: Country Code: Number:

Raw Data:

Reports

- [My Query History](#)
- [Recent Locations in My Region](#)
- [Worst GUIDs in My Region](#)
- [Worst IPs in My Region](#)

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
EL PASO DIVISION

FILED
2013 MAY 30 PM 4:30
CLERK, US DISTRICT COURT
WESTERN DISTRICT OF TEXAS
BY _____
Cause No. EP-11-CR-2728-KC

UNITED STATES OF AMERICA

§
§
§
§
§
§

v.

ANGEL OCASIO

MOTION TO QUASH SUBPOENA ISSUED PURSUANT TO
FEDERAL RULE OF CRIMINAL PROCEDURE 17

TO THE HONORABLE UNITED STATES DISTRICT COURT JUDGE:

COMES NOW Third-Party TLO, LLC (hereinafter "TLO"), by and through its undersigned counsel Christopher A. Antcliff, and files this, its Motion to Quash the subpoenas issued by Defendant Angel Ocasio ("Defendant") to William S. Wiltse ("Wiltse") and Derek A. Dubner, Esq. ("Dubner") and respectfully show the Court as follows:

I. INTRODUCTION

The subpoenas issued by Defendant to Wiltse and Dubner seek voluminous records and data relating to a highly proprietary law enforcement computer application known as the Child Protection System ("CPS") owned by TLO. CPS is used by governments around the world to track and stop the spread of child pornography. The subpoenas should be quashed not only because they are facially invalid, but also because they were issued for the improper purpose of discovery. Further, even if properly obtained and served, as instanter subpoenas they are oppressive given the scope and breadth of the requests. Finally, the materials sought are protected under the law enforcement privilege and trade secrets laws.

II. BACKGROUND

Defendant Angel Ocasio mailed instanter subpoenas duces tecum to Wiltse, an employee of TLO (*see* Subpoena, attached hereto as Exhibit 1) and to Dubner, counsel for TLO and registered agent for service of process (*see* Subpoena, attached hereto as Exhibit 2). These subpoenas seek various documents and technical information in TLO's possession relating to CPS. The subpoenas further require Wiltse and Dubner not to appear and/or testify in any court proceeding on any noticed date, but to send the documents directly to defense counsel.

The subpoenas seek broad categories of documents relating to CPS, including the source and object codes of the program. TLO vigorously protects its source code, and other aspects of CPS, as its value largely is derived from the fact that it is not widely accessible. If CPS were to become widely available, its efficacy in tracking users of child pornography would be greatly diminished. For example, if users became aware of how CPS operates, they could more easily detect when they are being investigated, making it harder for law enforcement officers to identify and track them. Additionally, providing access to anyone outside of law enforcement would compromise both present and ongoing criminal investigations around the world.

III. ARGUMENT

1. THE SUBPOENA AND ITS SERVICE ARE INVALID

Federal Rule of Criminal Procedure 17 provides in pertinent part:

- (a) Content. A subpoena must state the court's name and the title of the proceeding, include the seal of the court, and **command the witness to attend and testify at the time and place the subpoena specifies**. The clerk must issue a blank subpoena--signed and sealed--to the party requesting it, and that party must fill in the blanks before the subpoena is served.

...

(c) Producing Documents and Objects.

(1) In General. A subpoena may order the witness to produce any books, papers, documents, data, or other objects the subpoena

designates. The court may direct the witness to produce the **designated items in court** before trial or before they are to be offered in evidence. When the items arrive, the court may permit the parties and their attorneys to inspect all or part of them.

(d) Service. A marshal, a deputy marshal, or any nonparty who is at least 18 years old may serve a subpoena. The server must deliver a copy of the subpoena to the witness and must tender to the witness one day's witness-attendance fee and the legal mileage allowance. The server need not tender the attendance fee or mileage allowance when the United States, a federal officer, or a federal agency has requested the subpoena.

(emphasis added).

Taken in reverse order, the subpoenas were improperly served. Defense counsel mailed a copy of the subpoena to Wiltse and Dubner. Absent a witness's consent, such mailing constitutes improper service. *See* FED .R. CRIM. P. 17(d). However, this point is minor in comparison to other issues arising with the issuance and service of these two subpoenas.

First, the subpoenas are served upon persons unable to comply. TLO is the owner of CPS which is a highly proprietary law enforcement computer application protected under copyright law. *See* Affidavit of William Wiltse, attached hereto as Exhibit 3. While Mr. Wiltse is one of the developers of the software, he is only an employee of TLO and not an officer or director. He has no authority to legally produce the requested documents and information. Furthermore, Mr. Dubner, counsel for TLO and registered agent for service of process, was served as an individual as the

subpoena is directed to him and not TLO, LLC. Additionally, Mr. Dubner is not the custodian of records for TLO. As such, he does not have the legal authority to produce the requested documents.

Most importantly, Rule 17 requires that the subpoenas be issued in connection with a trial or other court hearing. In fact, the Rule 17 subpoenas as issued in this case, clearly state:

YOU ARE COMMANDED to appear in the United States district court at the time, date, and place shown below to testify in this criminal case. When you arrive, you must remain at the court until the judge or a court officer allows you to leave.

Nevertheless, the documents served by Defendant: (1) list no date or time for appearance at a court proceeding, but rather is listed as instant; and (2) do not designate that the items be delivered to the court. Rather the items are to be directly delivered to defense counsel.

It is well settled that Rule 17 does not authorize the government or the defense to subpoena a witness and require him to report at some place other than where the trial is to be held. *United States v. Standard Oil Co.*, 316 F.2d 884, 897 (7th Cir. 1963); *United States v. Hedge*, 462 F.2d 220 (5th Cir. 1972). It also is improper to direct the documents be delivered directly to defense counsel. *See United States v. Jenkins*, 895 F.Supp. 1389, 1394 (D.Hawai'i 1995) (finding that the court erred in allowing subpoenaed documents to be turned over directly to the defense and not to the court).

Even if Defendant could overcome these procedural errors, the subpoenas still should be quashed as they are issued for an improper purpose.

IV. THE SUBPOENA SEEKS DISCOVERY MATERIAL, NOT TRIAL MATERIAL

Although Rule 17 permits a party to a criminal proceeding to require production of documents or things via a subpoena, it is not intended to provide an additional means of discovery. *United States v. Nixon*, 418 U.S. 683, 699-700 (1963); *See also Bowman Dairy Co. v. United States*, 341 U.S. 214, 220. "[C]ourts must be careful that Rule 17(c) is not turned into a broad discovery device, thereby undercutting the strict limitation of discovery in criminal cases found in FED. R. CRIM. P. 16." *United States v. Salvagno*, 267 F. Supp. 2d 249 (N.D.N.Y. 2003). Thus, a party seeking documents pursuant to Rule 17 must establish:

(1) that the documents are evidentiary and relevant; (2) that they are not otherwise procurable reasonably in advance of trial by exercise of due diligence; (3) that the party cannot properly prepare for trial without such production and inspection in advance of trial and that the failure to obtain such inspection may tend unreasonably to delay the trial; and (4) that the application is made in good faith and is not intended as a general 'fishing expedition.'

Id., quoting *United States v. Nixon*, 418 U.S. 683,699-700 (1974). The effect of these requirements is that the party seeking documents bears the burden of proving that the information sought is relevant, admissible, and specific. *Id.*

Most importantly, a Rule 17 subpoena duces tecum may not be used to expand discovery in criminal cases. "While a Rule 17(c) subpoena duces tecum is a legitimate device to obtain evidentiary material, it was never intended to be a broad discovery device going beyond that which is required either by Rule 16 of the Federal Rules of Criminal Procedure or by Brady." *United States v. Edwards*, 191 F.Supp.2d 88, 89 (D.C. 2002), citing *United States v. Hardy*, 224 F.3d 752 (8th Cir. 2000); *United States v. Vanegas*, 112 F.R.D.

235, 238 (D.N.J. 1986); see *United States v. Nixon*, 777 F.2d 958, 968-69 (5th Cir. 1985); *United States v. Marcello*, 423 F.2d 993, 1006 (5th Cir.), cert. denied, 398 U.S. 959 (1970).

This is because a "Rule 17(c) subpoena reaches only evidentiary materials" -- not all discoverable materials. *United States v. Cuthbertson*, 651 F.2d 189, 195 (3rd Cir.) (citing *Bowman Dairy*, 71 S.Ct. at 679), cert. denied, 454 U.S. 1056 (1981). As such, a subpoena should be quashed where a party is attempting to improperly use it as a discovery tool.

As noted above, Federal Rule of Criminal Procedure 17 provides a means of obtaining admissible evidentiary material at trial. It is not intended as a basis to conduct broad searches for any possible information that may be of use to the defendant. See *Abdush-Shalcur*, 465 F.3d at 467; *United States v. King*, 164 F.R.D. 542, 546 (D. Kan. 1996) ("Rule 17 was not intended to provide the defendant a mechanism by which to troll the waters of the sea's otherwise undiscoverable material in the small hope that something beneficial might rise to the surface.") Indeed, the requests here resemble the type of discovery issued in civil cases, where discovery may be wide-ranging and searching, rather than discovery in a criminal case, which is limited to the specific materials permitted under Rule 16, plus what is required under the due process clause of the United States Constitution. See *United States v. Ramos*, 27 F.3d 65, 68 (3rd Cir. 1994) ("In contrast to the wide-ranging discovery permitted in civil cases, [Rule 16] delineates the categories of information to which defendants are entitled in pretrial discovery in criminal cases ...").

Subpoenas seeking broad categories of information or documents pursuant to Rule 17 are routinely quashed by federal courts, where no clear relevant or admissible

purpose is evident therein. See, .e.g., *United States v. Richardson*, 607 F.3d 357, 368 (4th Cir. 2010) (affirming quashing of defendant's subpoena upon finding that subpoena sought broad categories of documents from internet service provider in search of evidence supporting defense theory, and was therefore a fishing expedition); *United States v. Reed*, 726 F.2d 570, 577 (9th Cir. 1984) (affirming quashing of subpoena that requested broad categories of documents); *United States v. Daniels*, 95 F. Supp. 1160, 1169-70 (D. Kan. 2000) (refusing to issue subpoenas where requests were "extremely broad").

Courts have applied these standards to subpoenas duces tecum directed to third parties. See *United States v. Reyes*, 239 F.R.D. 591, 597 n. 1 (N.D. Cal. 2006). Here, Defendant cannot satisfy the requirements of Rule 17 with respect to the subpoenas he mailed to Wiltse and Dubner. Rather, Defendant is merely fishing for any possible support that might be beneficial to him. There cannot be, and is not a specific, discrete use at trial for all of the documents Defendant seeks from TLO, including training and instruction materials, testing and accreditation materials, and so forth. As such, the subpoenas should be quashed. *United States v. Dunn*, 2:09-CR-895 (D. Utah Oct. 20, 2011) [ECF Doc. 74] (quashing a similar subpoena served on TLO).

V. THE SUBPOENAS SEEK MATERIALS THAT ARE PROTECTED UNDER THE LAW ENFORCEMENT PRIVILEGE AND TRADE SECRETS LAWS

As an advanced law enforcement application for tracking online predators, information relating to the functions and uses of CPS is guarded with the highest level of caution. Access to CPS is only made available to specifically trained law enforcement

officers who have received instruction in its uses. Those officers who receive the training are licensed to use CPS only in the performance of their law enforcement work. Providing access to anyone outside of law enforcement would compromise both present and ongoing criminal investigations around the world.

Disclosure of the records and data requested in Defendant's subpoena would significantly degrade the usefulness of CPS as a worldwide investigative tool, as well as compromising numerous ongoing criminal investigations. A person with access to CPS or a working copy thereof could conceivably use it to learn a number of cutting-edge methods currently being used to enforce federal anti-child pornography laws. Access to such information makes it easier for criminals to evade investigative efforts, especially because CPS users can actually see which persons are under criminal investigation at any given time. Disclosure of these tools would create an enormous breach in the security of this information, and would damage the enforcement framework that has been constructed to combat the spread of child pornography.

In order to prevent such damage, the law recognizes a law enforcement privilege, which protects the techniques and methods of law enforcement from public disclosure. The privilege, which protects law enforcement techniques and procedures, sources, law enforcement personnel, and the privacy of individuals involved in investigations, has been well-recognized throughout the nation. *See In re Dep't. of Investigation of City of New York*, 856 F.2d 481,484 (2d Cir. 1988); *see also Hickey v. Columbus Consol. Gov't.*, No. 4:07-CV-96, 2008 WL 450561, *4 (Feb. 15, 2008) (discussing privilege); *United States v. Sam*, 2007 WL 2284602, *2 (D.S.D. Aug. 8, 2007) (quashing subpoena under law enforcement privilege). As disclosure of detailed information regarding the

CPS would degrade the effectiveness of global law enforcement efforts, the procedures and techniques requested by Defendant should not be disclosed.

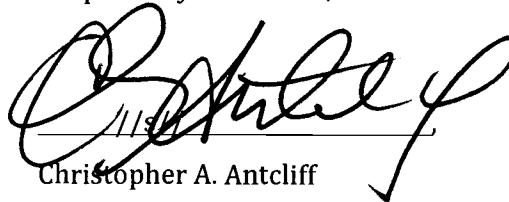
Further, all of the material requested by the subpoenas is held strictly confidential by TLO, and dissemination of such information would reduce its value. Therefore, the requested information holds trade secret status, and TLO requests the Court protect it accordingly. *See* FED. R. CRIM. P. 17(c)(2)

(providing that subpoena may be quashed if "compliance would be unreasonable or oppressive."); FED. R. CIV. P. 45(c)(3)(B)(i) (court may quash or modify subpoena if it requires "disclosing a trade secret or other confidential research, development, or commercial information."). Accordingly, the subpoenas should be quashed.

VI. CONCLUSION

For all of the reasons set forth above, the subpoenas issued by Defendant in this case are invalid, irrelevant, and overbroad, and seek privileged and protected information and material and TLO therefore requests that the Court quash the subpoenas.

Respectfully submitted,



Christopher A. Antcliff

Tx. Bar No. 00793269

221 N. Kansas, Ste. 1201

El Paso, Texas 79901

Tel: (915) 533-1221

Fax: (915) 533-1225

CERTIFICATE OF SERVICE

I hereby certify that on the 30th day of May, 2013, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system which will send notification of such filing to all counsel of record in this cause.



Chris Antcliff

AO 89 (Rev. 08/09) Subpoena to Testify at a Hearing or Trial in a Criminal Case

UNITED STATES DISTRICT COURT

for the

Western District of Texas

United States of America)

v.)

ANGEL OCASIO)

Case No. EP-11-CR-2728-KC

Defendant)

SUBPOENA TO TESTIFY AT A HEARING OR TRIAL IN A CRIMINAL CASE

To: DUBNER, DEREK A., ESQ.
c/o TLO, LLC
4530 Conference Way South
Boca Raton, FL 33431

YOU ARE COMMANDED to appear in the United States district court at the time, date, and place shown below to testify in this criminal case. When you arrive, you must remain at the court until the judge or a court officer allows you to leave.

Place of Appearance: Federal Public Defender 700 E. San Antonio, Ste. D401 El Paso, TX 79901	Courtroom No.: Instanter
	Date and Time:

You must also bring with you the following documents, electronically stored information, or objects (blank if not applicable):

Please see attached requested information:

(SEAL)

Date: 5/1/13

CLERK OF COURT

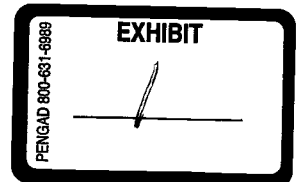
WILLIAM G. PUTNEY

Signature of Clerk or Deputy Clerk

The name, address, e-mail, and telephone number of the attorney representing (name of party)

Angel Ocasio, who requests this subpoena, are:

Michael Gorman, Assistant Federal Public Defender, 700 E. San Antonio, Ste. D-401, El Paso, TX 79901;
915-534-6525.



AO 89 (Rev. 08/09) Subpoena to Testify at a Hearing or Trial in a Criminal Case (Page 2)

Case No. EP-11-CR-2728-KC

PROOF OF SERVICE

This subpoena for *(name of individual and title, if any)* _____
was received by me on *(date)* _____.

I served the subpoena by delivering a copy to the named person as follows: _____
VIA CERT MAIL RRR
7006215000491009828 on *(date)* 5-1-13 ; or

I returned the subpoena unexecuted because: _____

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also
tendered to the witness fees for one day's attendance, and the mileage allowed by law, in the amount of
\$ _____.

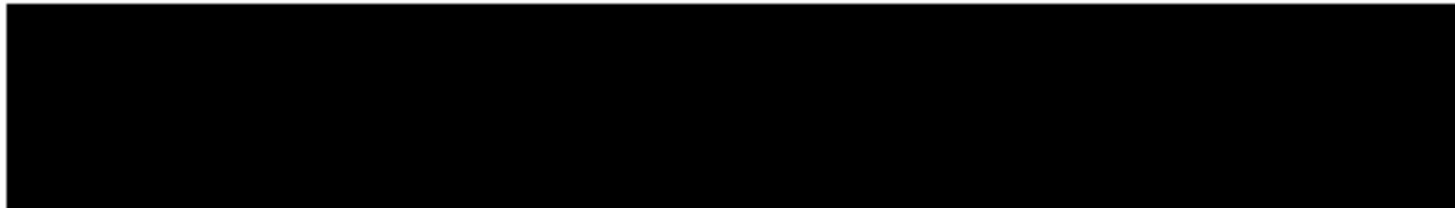
My fees are \$ _____ for travel and \$ _____ for services, for a total of \$ 0.00.

I declare under penalty of perjury that this information is true.

Date: 5-1-13

C.H. _____
Server's signature

C. Hernandez _____
Printed name and title



Additional information regarding attempted service, etc:

U.S. v. Angel Ocasio
EP-11-CR-2728-KC

SUBPOENA ATTACHMENT A:

Please provide the following:

1. The source and object code, to include all non-compileable programmer comments provided in the same, of the application known as Child Protection System, as that System was implemented and in effect on April 11, 2011.
2. The source and object code of any application called by the Child Protection System when executing, to include any helper application. In the event any application called is non-proprietary and commercially available, identify the application and version called by the System in effect on April 11, 2011. If the application called is not commercially available, provide the complete source and object code, along with programmer comments, in effect on April 11, 2011.
3. Complete revision history of the Child Protection System and corresponding changes implemented by individual System revisions.
4. Project Management documentation utilized in the design and revision of Child Protection System, to include requirements management if utilized.
5. Any documentation describing and addressing known bugs or failures in the Child Protection System, along with corrective measures taken and dates such measures were implemented, if applicable.
6. FAQs, if provided to law enforcement officers or agents utilizing the System.

Please provide the above by attachment instanter to e-mail address: [REDACTED] or by mail in a generally accepted digital format to Michael Gorman, Assistant Federal Public Defender, 700 E. San Antonio, Ste. D401, El Paso, TX 79901.

AO 89 (Rev. 08/09) Subpoena to Testify at a Hearing or Trial in a Criminal Case

UNITED STATES DISTRICT COURT

for the

Western District of Texas

United States of America)

v.)

ANGEL OCASIO)

Case No. EP-11-CR-2728-KC

Defendant)

SUBPOENA TO TESTIFY AT A HEARING OR TRIAL IN A CRIMINAL CASE

To: William S. Wiltse
4530 Conference Way South
Boca Raton, FL 33431

YOU ARE COMMANDED to appear in the United States district court at the time, date, and place shown below to testify in this criminal case. When you arrive, you must remain at the court until the judge or a court officer allows you to leave.

Table with 2 columns: Place of Appearance (Federal Public Defender, 700 E. San Antonio, Ste. D401, El Paso, TX 79901) and Courtroom No. (Instantanter). Date and Time field is empty.

You must also bring with you the following documents, electronically stored information, or objects (blank if not applicable):

Please see attached requested information:

(SEAL)

Date: 5/1/13

CLERK OF COURT

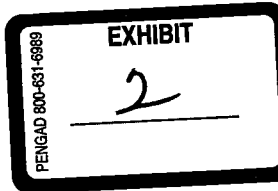
WILLIAM G. PISTONICKI

Signature of Clerk or Deputy Clerk

The name, address, e-mail, and telephone number of the attorney representing (name of party)

Angel Ocasio, who requests this subpoena, are:

Michael Gorman, Assistant Federal Public Defender, 700 E. San Antonio, Ste. D-401, El Paso, TX 79901; 915-534-6525.



U.S. v. Angel Ocasio
EP-11-CR-2728-KC

SUBPOENA ATTACHMENT A:

Please provide the following:

1. The source and object code, to include all non-compilable programmer comments provided in the same, of the application known as Child Protection System, as that System was implemented and in effect on April 11, 2011.
2. The source and object code of any application called by the Child Protection System when executing, to include any helper application. In the event any application called is non-proprietary and commercially available, identify the application and version called by the System in effect on April 11, 2011. If the application called is not commercially available, provide the complete source and object code, along with programmer comments, in effect on April 11, 2011.
3. Complete revision history of the Child Protection System and corresponding changes implemented by individual System revisions.
4. Project Management documentation utilized in the design and revision of Child Protection System, to include requirements management if utilized.
5. Any documentation describing and addressing known bugs or failures in the Child Protection System, along with corrective measures taken and dates such measures were implemented, if applicable.
6. FAQs, if provided to law enforcement officers or agents utilizing the System.

Please provide the above by attachment instanter to e-mail address: [REDACTED] or by mail in a generally accepted digital format to Michael Gorman, Assistant Federal Public Defender, 700 E. San Antonio, Ste. D401, El Paso, TX 79901.

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
EL PASO DIVISION**

UNITED STATES OF AMERICA

v.

ANGEL OCASIO

20130530 10:00:00 AM

Cause No. EP-11-CR-2728-KC

AFFIDAVIT OF WILLIAM S. WILTSE

Before me, the undersigned authority, personally appeared WILLIAM S. WILTSE, who, being by me duly sworn, deposed as follows:

“My name is WILLIAM S. WILTSE, I am over the age of 21 years, of sound mind, capable of making this affidavit, and have personal knowledge of the facts herein stated:

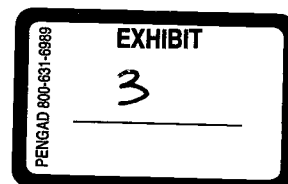
“1. I currently reside in Palm Beach County, Florida.

“2. I am a former police detective for the City of Salem, Oregon. I worked as a police officer in the State of Oregon for the past 18 years, during which time I conducted criminal investigations into the sexual abuse and exploitation of children.

“3. I am currently employed by TLO, LLC, as its Security Director over Law Enforcement Systems. I am neither an officer nor a director of TLO, LLC.

“4. TLO is a private company located in Boca Raton, Florida, that provides software and databases for the law enforcement community and other private investigators.

“5. TLO also manages the licensing for, and access to, the CPS, which is an application developed by TLO to allow law enforcement officers around the world to track the use and distribution of child pornography online.



“6. CPS is an advanced law enforcement method for identifying images of child pornography across this network, and tracking users who offer them for downloading on the network. The toolkit allows an investigator to search for such files in a given jurisdiction, and to mark such files to alert other investigators that a given computer is under investigation. This function allows enforcement officers to coordinate their efforts and prevents duplication of effort (where otherwise multiple investigators might pursue the same user).

“7. Because it is an advanced application for tracking online predators, information relating to the functions and uses of the CPS is guarded with the highest level of caution. Providing access to anyone outside of law enforcement would compromise both present and ongoing criminal investigations around the world.

“8. CPS is only made available to specifically trained law enforcement officers who have received intensive instruction in its uses. Those officers who receive the license are permitted to use CPS only in performance of their law enforcement work.

“9. CPS is a proprietary computer application protected under copyright law.

“10. Investigators do not receive the source code for CPS as part of their training, but only the application itself. One cannot access the source code simply by using the application.

“11. TLO vigorously protects the source code of CPS, as its value is largely derived from the fact that it is not widely accessible by the public. If CPS were to become widely available, its efficacy in tracking users of child pornography would be greatly diminished. For example, if users became aware of how CPS operates, they could more easily detect when they are being investigated, making it harder for law enforcement

officers to identify and track them.

I declare under criminal penalty of perjury that the foregoing is true and correct.

FURTHER SAYETH AFFIANT NOT.

DATED this 30th day of May, 2013.


WILLIAM S. WILTSE

From: Carly Asher Yoost <[REDACTED]>
Sent: Wednesday, January 23, 2019 7:50 PM
To: Sarah St.Vincent <[REDACTED]>
Subject: Re: Request for comment from Human Rights Watch

Sarah,

At Child Rescue Coalition we are dedicated to putting a stop to the horrible epidemic of child sexual abuse. We believe every child's innocence should be protected. With the outpour of support from our donors and the great dedication of law enforcement, we have been able to aid in the arrest of over 10,900 dangerous child sex offenders and the rescue of over 2,500 child victims. Knowing that each offender typically abuses 50-150 victims in the course of their lifetime, we have undoubtedly prevented thousands of children from ever becoming victims in the first place. When children are victimized their dignity and chance at a successful adulthood is stripped from them. We know that child sex abuse victims are worth fighting for.

The role that Child Rescue Coalition plays to aid in this fight is that we are successfully identifying computers that are responsible for the trade of illegal child abuse material. Our CPS technology has been tested extensively by courts and by third party companies and has been found 100% of the time to not be violating any privacy rights or concerns. We track activity and files traded in open networks and public forums. We appreciate your interest in our organization. As a policy, we do not publicly share details of how we identify sex offenders online as we do not want predators to learn better ways to hide their illegal activity. If you wish to support Child Rescue Coalition, please do so by visiting our website ChildRescueCoalition.org. We hope you join our fight in keeping the world a safer place for our children.

Carly Asher Yoost Founder & CEO, Child Rescue Coalition

Phone: [REDACTED]
Mobile: [REDACTED]
Email: [REDACTED]
Address: [4530 Conference Way S](#)
[Boca Raton, FL 33431](#)

MICHAEL K. JEANES, CLERK
BY
A. GAMBLE, FILED
17 NOV 28 PM 1:03

IN THE SUPERIOR COURT OF THE STATE OF ARIZONA
MARICOPA COUNTY

State of Arizona,

Plaintiff

v.

Thomas W. Tolworthy (001),

Defendant

No. CR2015-119746-001

**MOTION OF UNIVERSITY OF MASSACHUSETTS TO RECONSIDER
ORDER OF 19 SEPTEMBER 2017**

Now comes the University of Massachusetts (“the University”), and hereby respectfully moves the court to reconsider its order of September 19, 2017 for the reasons outlined below.

On September 19, 2017, the Hon. Mark H. Brain ordered the University of Massachusetts Amherst produce the computer software Torrential Downpour to Maricopa County Public Defender Jessica Spargo. The University respectfully requests that the court reconsider its order for the reasons outlined below. As grounds for this Motion, the University states the following.

1. The order does not comply with the Uniform Act To Secure the Attendance of Witnesses From Without a State in Criminal Proceedings, codified in Sections 13A to 13D of chapter 233 of the Massachusetts General Laws, and its cognate Arizona statute at A.R.S. §§ 13-4091 to 13-4096. The Uniform Act requires that (1) a judge of the requesting state must certify that a

criminal proceeding or a Grand Jury investigation is pending in that state, (2) the requesting state judge must also certify that a Massachusetts resident is a material and necessary witness; (3) after receiving the out-of-state certificate, a Massachusetts Superior Court judge sitting in the county, or the justice or a special justice of the district court in the judicial district, in which such person is located, must hold a hearing to determine whether compelling the witness' attendance will cause him or her undue hardship and to determine whether the Massachusetts witness is material and necessary to the out-of-state proceeding; and (4) if the Massachusetts judge or justice so determines he shall issue a summons, including either a subpoena or order requiring the appearance of a witness in the requesting state. Massachusetts case law has analogized the power to compel the production of documents to the power to compel the testimony of a witness, and would likely regard the Order in this case to fall within the Uniform Act. See In re Grand Jury of State of N.Y., 8 Mass. App. Ct. 760, 762 (1979). It is the University's position that the intent and effect of the Uniform Act is to allow the University a hearing before a Massachusetts judge before it is required to produce valuable intellectual property held by the institution or its faculty.

2. Providing the intellectual property to the defendant in this case will destroy its value to the University and its faculty researcher. The University has received funding from the U.S. Department of Justice since 2008 for the development of software tools to permit detection of peer-to-peer sharing of child pornography. Most recently, the University's faculty researcher has conducted this work on a \$440,000 annual grant from the Federal Bureau of Investigation. Revealing the software code could diminish its value as a law enforcement tool and potentially end funding for a valuable line of research for the University and its faculty. Under federal

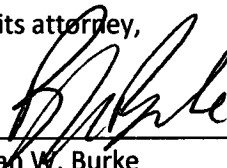
regulations copyright to the software is held by the University or faculty member, subject to a nonexclusive license to the DOJ. See 2 CFR 200.315 and sections cited therein. Thus far, the University has never given out the source code to the Software, except to the project manager at the FBI for validation purposes.

3. Finally, related to the above, the University points out that the Software serves an important law enforcement purpose. Currently, the software is in use by the FBI and in every state in the US, including all 61 instances of the Internet Crimes Against Children Task Force. Releasing it to public view would frustrate public policy and impede law enforcement's ability to deter peer-to-peer sharing of child pornography. The University believes that before it is required to release the software beyond its distribution to date to law enforcement, the FBI, as funding agency, should be given an opportunity to weigh in on the matter.

CONCLUSION

WHEREFORE, for the above-stated reasons, the University of Massachusetts respectfully requests that this court reconsider its order compelling the University to produce the software to the defendant in this case.

Respectfully submitted,
UNIVERSITY OF MASSACHUSETTS,
By its attorney,



Brian W. Burke
Senior Counsel – Amherst
BBO#633048
309 Whitmore Administration Building
University of Massachusetts
181 Presidents Drive
Amherst, MA 01003
Tel: 413/545-2204
bwburke@umass.edu

Dated: November 20, 2017

CERTIFICATE OF SERVICE

I, Brian W. Burke, counsel for the University of Massachusetts, hereby certify that on November 20, 2017, a true copy of the above Motion for Reconsideration was served by U.S. Mail upon JESSICA SPARGO, MARICOPA COUNTY PUBLIC DEFENDER, 620 W. JACKSON STREET, SUITE 4015, PHOENIX, AZ 85003.

A handwritten signature in black ink, appearing to read "B. Burke", is written over a horizontal line.

Brian W. Burke

MICHAEL K. JEANES, CLERK
BY *E. Masio* DEP
FILED

WILLIAM G MONTGOMERY
MARICOPA COUNTY ATTORNEY

15 MAY -8 PM 4: 42

Margaret Wu
Deputy County Attorney
Bar ID #: 024805
301 W. Jefferson, 5th Floor
Phoenix, AZ 85003
Telephone: (602) 506-8556
mcaosvd@mcao.maricopa.gov
MCAO Firm #: 00032000
Attorney for Plaintiff

DR 201500747329 - Phoenix Police Department
1553069

IN THE SUPERIOR COURT OF THE STATE OF ARIZONA

IN AND FOR THE COUNTY OF MARICOPA

THE STATE OF ARIZONA,

Plaintiff,

vs.

THOMAS WILLIAM TOLWORTHY,

Defendant.

CR2015-119746-001

INDICTMENT
640 GJ 226

**COUNT 1: SEXUAL EXPLOITATION OF A
MINOR, A CLASS 2 FELONY DANGEROUS
CRIME AGAINST CHILDREN (THOMAS
WILLIAM TOLWORTHY)**

**COUNT 2: SEXUAL EXPLOITATION OF A
MINOR, A CLASS 2 FELONY DANGEROUS
CRIME AGAINST CHILDREN (THOMAS
WILLIAM TOLWORTHY)**

**COUNT 3: SEXUAL EXPLOITATION OF A
MINOR, A CLASS 2 FELONY DANGEROUS
CRIME AGAINST CHILDREN (THOMAS
WILLIAM TOLWORTHY)**

**COUNT 4: SEXUAL EXPLOITATION OF A
MINOR, A CLASS 2 FELONY DANGEROUS
CRIME AGAINST CHILDREN (THOMAS
WILLIAM TOLWORTHY)**

COUNT 5: SEXUAL EXPLOITATION OF A MINOR, A CLASS 2 FELONY DANGEROUS CRIME AGAINST CHILDREN (THOMAS WILLIAM TOLWORTHY)

COUNT 6: SEXUAL EXPLOITATION OF A MINOR, A CLASS 2 FELONY DANGEROUS CRIME AGAINST CHILDREN (THOMAS WILLIAM TOLWORTHY)

COUNT 7: SEXUAL EXPLOITATION OF A MINOR, A CLASS 2 FELONY DANGEROUS CRIME AGAINST CHILDREN (THOMAS WILLIAM TOLWORTHY)

COUNT 8: SEXUAL EXPLOITATION OF A MINOR, A CLASS 2 FELONY DANGEROUS CRIME AGAINST CHILDREN (THOMAS WILLIAM TOLWORTHY)

COUNT 9: SEXUAL EXPLOITATION OF A MINOR, A CLASS 2 FELONY DANGEROUS CRIME AGAINST CHILDREN (THOMAS WILLIAM TOLWORTHY)

COUNT 10: SEXUAL EXPLOITATION OF A MINOR, A CLASS 2 FELONY DANGEROUS CRIME AGAINST CHILDREN (THOMAS WILLIAM TOLWORTHY)

The Grand Jurors of Maricopa County, Arizona, accuse THOMAS WILLIAM TOLWORTHY, on May 8, 2015, charging that in Maricopa County, Arizona:

COUNT 1:

THOMAS WILLIAM TOLWORTHY, on or between November 1, 2014 and May 1, 2015, knowingly did distribute, transport, exhibit, receive, sell, purchase, electronically transmit, possess, or exchange any visual depiction in which a minor under fifteen years of age is engaged in exploitive exhibition or other sexual conduct, (to witt:magn-03-043.jpg) in violation of A.R.S. §§ 13-3553, 13-3551, 13-3821, 13-705, 13-701, 13-702, and 13-801.

COUNT 2:

THOMAS WILLIAM TOLWORTHY, on or between November 1, 2014 and May 1, 2015, knowingly did distribute, transport, exhibit, receive, sell, purchase, electronically transmit, possess, or exchange any visual depiction in which a minor under fifteen years of age is

engaged in exploitive exhibition or other sexual conduct, (to witt:magn-03-067.jpg) in violation of A.R.S. §§ 13-3553, 13-3551, 13-3821, 13-705, 13-701, 13-702, and 13-801.

COUNT 3:

THOMAS WILLIAM TOLWORTHY, on or between November 1, 2014 and May 1, 2015, knowingly did distribute, transport, exhibit, receive, sell, purchase, electronically transmit, possess, or exchange any visual depiction in which a minor under fifteen years of age is engaged in exploitive exhibition or other sexual conduct, (to witt:magn-05-036.jpg) in violation of A.R.S. §§ 13-3553, 13-3551, 13-3821, 13-705, 13-701, 13-702, and 13-801.

COUNT 4:

THOMAS WILLIAM TOLWORTHY, on or between November 1, 2014 and May 1, 2015, knowingly did distribute, transport, exhibit, receive, sell, purchase, electronically transmit, possess, or exchange any visual depiction in which a minor under fifteen years of age is engaged in exploitive exhibition or other sexual conduct, (to witt:ml32a050.jpg) in violation of A.R.S. §§ 13-3553, 13-3551, 13-3821, 13-705, 13-701, 13-702, and 13-801.

COUNT 5:

THOMAS WILLIAM TOLWORTHY, on or between November 1, 2014 and May 1, 2015, knowingly did distribute, transport, exhibit, receive, sell, purchase, electronically transmit, possess, or exchange any visual depiction in which a minor under fifteen years of age is engaged in exploitive exhibition or other sexual conduct, (to witt:ml32a095.jpg) in violation of A.R.S. §§ 13-3553, 13-3551, 13-3821, 13-705, 13-701, 13-702, and 13-801.

COUNT 6:

THOMAS WILLIAM TOLWORTHY, on or between November 1, 2014 and May 1, 2015, knowingly did distribute, transport, exhibit, receive, sell, purchase, electronically transmit, possess, or exchange any visual depiction in which a minor under fifteen years of age is engaged in exploitive exhibition or other sexual conduct, (to witt:4yo girl spread legs. jpg) in violation of A.R.S. §§ 13-3553, 13-3551, 13-3821, 13-705, 13-701, 13-702, and 13-801.

COUNT 7:

THOMAS WILLIAM TOLWORTHY, on or between November 1, 2014 and May 1, 2015, knowingly did distribute, transport, exhibit, receive, sell, purchase, electronically transmit, possess, or exchange any visual depiction in which a minor under fifteen years of age is engaged in exploitive exhibition or other sexual conduct, (to witt:babyea.1t.jpg.jpg) in violation of A.R.S. §§ 13-3553, 13-3551, 13-3821, 13-705, 13-701, 13-702, and 13-801.

COUNT 8:

THOMAS WILLIAM TOLWORTHY, on or between November 1, 2014 and May 1, 2015, knowingly did distribute, transport, exhibit, receive, sell, purchase, electronically transmit, possess, or exchange any visual depiction in which a minor under fifteen years of age is engaged in exploitive exhibition or other sexual conduct, (to witt:babymario16.jpg) in violation of A.R.S. §§ 13-3553, 13-3551, 13-3821, 13-705, 13-701, 13-702, and 13-801.


COUNT 9:

THOMAS WILLIAM TOLWORTHY, on or between November 1, 2014 and May 1, 2015, knowingly did distribute, transport, exhibit, receive, sell, purchase, electronically transmit, possess, or exchange any visual depiction in which a minor under fifteen years of age is engaged in exploitive exhibition or other sexual conduct, (to witt:Pedo Baby 03 – 2 yo Photos 53.jpg) in violation of A.R.S. §§ 13-3553, 13-3551, 13-3821, 13-705, 13-701, 13-702, and 13-801.

COUNT 10:

THOMAS WILLIAM TOLWORTHY, on or between November 1, 2014 and May 1, 2015, knowingly did distribute, transport, exhibit, receive, sell, purchase, electronically transmit, possess, or exchange any visual depiction in which a minor under fifteen years of age is engaged in exploitive exhibition or other sexual conduct, (to witt:Pedo Baby 03 – 2 yo Photos 56.jpg) in violation of A.R.S. §§ 13-3553, 13-3551, 13-3821, 13-705, 13-701, 13-702, and 13-801.


WILLIAM G MONTGOMERY
MARICOPA COUNTY ATTORNEY


Margaret Wu
Deputy County Attorney

rg

A True Bill
("A True Bill")

Date: May 8, 2015


FOREPERSON OF THE GRAND JURY

**IN THE SUPERIOR COURT OF THE STATE OF ARIZONA
IN AND FOR THE COUNTY OF MARICOPA**

STATE OF ARIZONA,
Plaintiff,
v.
THOMAS TOLWORTHY,
Defendant.

Case No. CR2015-119746-001 DT

AFFIDAVIT OF TAMI LOEHRS

I, TAMI L. LOEHRS, hereby declare as follows:

1. I am a computer forensics expert and owner of Loehrs& Associates, LLC (formerly Law2000, Inc.) a firm specializing in computer forensics. My offices are located at 3037 West Ina, Suite 121, Tucson, Arizona 85741. I am competent to testify and the matters contained herein are based on my own personal knowledge.

2. I have been working with computer technology for over 25 years and I hold a Bachelor of Science in Information Systems. I have completed hundreds of hours of forensics training including courses with Guidance Software and Access Data. I am an EnCase Certified Examiner (EnCE), an Access Data Certified Examiner (ACE), a Certified Computer Forensic Examiner (CCFE) and a Certified Hacking Forensic Investigator (CHFI). I have conducted hundreds of forensics exams on thousands of pieces of evidence including hard drives, cell phones, removable storage media and other electronic devices. I have conducted seminars on Computer Forensics and Electronic Discovery throughout the United States. In addition, I hold a Private Investigator Agency License in the State of Arizona which requires a minimum of

6,000 hours investigative experience. My Curriculum Vitae is attached hereto and updated versions may be downloaded from the Loehrs & Associates website at www.ForensicsExpert.net.

3. I have been the computer forensics expert for the defense on over 250 child pornography cases throughout the United States, Puerto Rico, Marianna Islands, Canada and England since the year 2000 and have testified over one hundred times in State, Federal and international Courts.

4. I have been retained as a computer forensics expert by Craig Gillespie, counsel for Defendant Thomas Tolworthy, for the purpose of assisting with matters related to the searching, collecting, analyzing and producing of electronic evidence in this matter.

5. I have reviewed discovery materials produced by the State of Arizona including, but not limited to, Phoenix Police Department Report dated April 29, 2015 (0001-0004), Digital Evidence Examination Report prepared by Detective Haddad, the Indictment, Grand Jury Transcript dated May 8, 2015 and Transcript of Interview of Jimmie John Daniels dated July 26, 2016.

6. According to the Phoenix Police Department Report (0002), this case originated on February 1, 2015 when the IP address 68.109.164.156 was identified by SA Jimmie John Daniels of the FBI as sharing 14 pieces of a 685 piece torrent with the info hash 817E0637DD4BDFDB4BC032408DA650391D8FD609. Those 14 pieces contained 457 complete files, some of which were identified as child pornography.

7. In order to understand the complexities of the undercover investigation that identified Mr. Tolworthy in this matter, it is imperative to understand the difference between

the “BitTorrent network”, a “torrent”, an “info hash” and an actual image or video that depicts child pornography.

8. The “BitTorrent network” is essentially a protocol or set of rules that allows users to download and upload parts of files from many different users which are then rebuilt into the whole files. This means that someone downloading files on the BitTorrent network may get small pieces of those files from many different computers to rebuild the file on their own computer. This also means that a user with an empty file or a small fragment of a file may still be identified on the BitTorrent network as a download candidate for the whole file even if they don’t possess the whole file.

9. A “torrent” is a text file proprietary to the BitTorrent network that contains instructions for torrent software, such as uTorrent or BitLord, on how to download a file or sets of files on the BitTorrent network. Torrent files do not contain user data, such as images or videos, but rather an index containing information about the files associated with that torrent including but not limited to, names of the files instructed to download, the torrent author, the date the author of the torrent created the file, the number of files the torrent is set to download, and the URLs tracking the torrent activity.

10. An “info hash” is a mathematical algorithm or hash value that uniquely identifies the “torrent” on the BitTorrent network. Although it has been described as synonymous with a fingerprint, the info hash only identifies the torrent itself, not the actual files the torrent would download if parsed.

11. If Person A downloads a torrent to his computer, the info hash and file names of every file associated with that torrent would be cached to his computer. If that torrent is never parsed, the associated files are never actually downloaded to the computer and Person A does

not possess those files. However, that torrent may still be read by torrent software and falsely advertised on the BitTorrent network as a download candidate for all of the associated files even though none of the files exist. If Person B tries to download the same torrent on the BitTorrent network, Person A will be listed as a download candidate. However, the files downloaded to Person B's computer will not come from Person A, rather, the bits and pieces will come from other users on the BitTorrent network who actually have the files.

12. During my independent computer forensics examination of approximately eleven evidence items seized from Mr. Tolworthy, I was unable to locate the torrent, the info hash or the files of child pornography identified during the undercover investigation. In addition, the torrent, the info hash and the files of child pornography were not found by the State's forensic examiner either.

13. According to the interview of SA Daniels, the information that a torrent containing files of child pornography was available at IP address 68.109.164.156 was actually obtained by automated law enforcement sensitive software that monitors peer-to-peer file sharing networks. That software was identified by SA Daniels as Torrential Downpour (Transcript of Interview, page 4).

14. In my experience on hundreds of cases throughout the country involving law enforcement's on-line undercover investigations of peer-to-peer file sharing networks, I am familiar with the use of the Torrential Downpour software. I am also familiar with issues that have come to light with regard to the accuracy and reliability of law enforcement's proprietary software and whether the information obtained is publicly available. However, based on my personal knowledge working on these cases and listening to law enforcement testimony, the Torrential Downpour software has never been tested and validated. It is critical to Mr.

Tolworthy's defense to understand how this software functions in order to determine its reliability and accuracy in identifying files allegedly belonging to Mr. Tolworthy when none of the files, the torrent nor the info hash were found on any of his computers.

15. In my forensic training, some of which has come directly from law enforcement, I have been taught that I cannot rely on a tool (software) that has not been tested and validated by me and is not available for testing and validation by my industry peers. This is why most forensic examiners use tools like EnCase and FTK because they are industry standard tools that are available for testing and validation by anyone and, as such, have been accepted by the Courts as viable tools. However, even those tools have been proven to produce inaccurate and unreliable data at times which has only been discovered through the ability to test and validate them.

16. The biggest challenge with developing an accurate tool is the diversity of data being collected and analyzed. This is why even tools like EnCase and FTK sometimes produce inaccurate and unreliable results. No two computer systems are identical. Computers are installed with different operating systems and there are hundreds of different versions of the same operating system, some are updated regularly and some are not updated at all. Those operating systems have thousands of different settings that can make each system unique in how it functions and records data. Within those operating systems a user can install millions of different software applications from large commercially produced software to small home-made software applications. Software applications may have bugs, data can be corrupted or incomplete, computers can be infected with viruses, Trojans and other malware. All of these variables have an effect on how that data is collected, analyzed and documented by a tool. While a tool may provide accurate information on an updated Windows system without any


malware, the same tool may yield false results on a system that has not been updated and is infested with viruses.

17. When talking specifically about P2P software, there are hundreds of versions of file sharing software applications that users can download from the Internet. Some are free and some are paid for. Some are updated regularly with new versions, some are not. Some of those applications are open source, meaning the user can actually modify the source code of the application allowing it to function differently than the exact same piece of software installed on another computer. I have personally been researching, testing and analyzing P2P file sharing software available to the public for over ten years including, but not limited to, LimeWire, FrostWire, Bearshare, Ares, BitTorrent, eMule, Phex and Shareaza. What I have discovered in all of these programs is that they can contain bugs, they do not always function as intended and the data reported by these applications is not always accurate or reliable. In that regard, any tool used to collect, analyze and document data associated with these applications may also be inaccurate and unreliable.

18. For all of the reasons stated above, and under general scientific principles, it is my opinion that the software relied upon during the undercover investigation needs to be tested and validated by a qualified third-party to determine its functionality, accuracy and reliability.

19. I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Dated: 10/5/14


Tami L. Lochrs

SUPERIOR COURT OF ARIZONA
MARICOPA COUNTY

CR2015-005499-001 DT
CR2015-119746-001 DT

02/17/2017

HONORABLE MARK H. BRAIN

CLERK OF THE COURT
M. Askew
Deputy

STATE OF ARIZONA

REBECCA KATHLEEN JONES

v.

THOMAS W TOLWORTHY (001)

CRAIG C GILLESPIE

TRIAL CONTINUANCE

Prior to commencement of today's proceedings, Defendant's exhibits 1-4 are marked for identification. All exhibits are marked under CR2015-005499-001.

1:33 p.m.

Courtroom CCB 1201

State's Attorney:	Rebecca Jones
Defendant's Attorney:	Craig Gillespie
Defendant:	Present

Court Reporter, Lisa Bradley, is present.

A record of the proceedings is also made digitally.

This is the time set for Evidentiary Hearing on Defendant's Motion to Suppress and Final Trial Management Conference.

SUPERIOR COURT OF ARIZONA
MARICOPA COUNTY

CR2015-005499-001 DT
CR2015-119746-001 DT

02/17/2017

This matter came before the Court for a hearing on two motions, both of which were filed on December 5, 2016: (1) Defendant's Motion for Disclosure of Software; and (2) Defendant's Motion to Suppress and for *Franks* Hearing.

Both motions are DENIED (the first with caveats). By way of brief explanation, the Court notes the following.

Defendant's Motion for Disclosure of Software fails (and is therefore DENIED) because the materials sought are not in the possession or control of the prosecutor or a law enforcement agency under the prosecutor's direction or control, as required by Rule 15.1(f). Instead, Special Agent Daniels of the FBI has a licensed copy of the software. Agent Daniels is cooperating with the prosecutor, but he is not under the direction or control of the Maricopa County Attorneys' Office (as one might imagine, he answers to someone else). That said, given that the only evidence supporting Counts 6-10 was generated by the software program (stated another way, the images forming the basis for Counts 6-10 was not found on defendant's computer), it does appear that defendant has a substantial need for the software, subject to the balancing required by Rule 15.1(g). Defense counsel shall submit an order for production of the software to the Court for signature, and shall be responsible for serving the "owner" of the software (that is, the person or entity with lawful authority to distribute the software as it chooses). That order shall provide the "owner" with 20 days from the date of service to produce the materials or file an objection under Rule 15.1(g).

Defendant's Motion for a *Franks* hearing is DENIED. As noted by the State, a prerequisite to a full-blown *Franks* hearing challenging a warrant is a substantial preliminary showing that: (1) the affiant made a false statement with the requisite mental state; and (2) excluding the false statement, the remainder of the information is insufficient to support a probable cause finding. The Court doesn't believe defendant has met the first prong, but even setting aside the challenged information, the affidavit discloses: (1) none of the ordinary occupants of the Peterson residence had the knowledge or ability to access the files; (2) the Petersons' working computer did not have any files of interest when inspected; (3) defendant lived at the Peterson home during the period at issue and was given the wifi password for the home; (4) defendant had both computer equipment and an IT background; and (5) defendant spent the majority of his time on his laptop and was "unusual" in his behaviors. *See* Warrant at bates stamp 0084. This information, standing alone, is easily sufficient to support a probable cause finding for a warrant.

Finally, the Court rejects the claim that the warrant was overbroad. The principle cases cited by defendant are easily distinguishable. *United States v. Winn*, 79 F. Supp. 3d 904 (S.D. Ill. 2015) arose from a claim that defendant was masturbating near a public pool while taking

SUPERIOR COURT OF ARIZONA
MARICOPA COUNTY

CR2015-005499-001 DT
CR2015-119746-001 DT

02/17/2017

pictures or videos of children on his cell phone on a particular date. It would have been an easy matter to limit the warrant to videos or pictures on that date. *Oregon v. Mansor*, 279 Or. App. 778 (2016) likewise involved a search of a computer after a father indicated he had researched specific issues on a particular day after his infant son quit breathing. Again, it would have been easy to limit the warrant. This case, on the other hand, more closely resembles *United States v. Lacy*, 119 F.3d 742 (9th Cir. 1997), which allowed a broader warrant. After all, the investigation in this case had revealed that child pornography was being *shared from* the Peterson's internet protocol address using specific software. The warrant at issue was reasonably tailored to gather evidence of that crime. It matters little that defendant's the desktop computer had not been used for some period. After all, in order to share files, one must first possess them (at an earlier period), and it is common knowledge that digital files can be transferred from computer to computer through memory sticks, etc.

Upon agreement of the parties and good cause appearing based on the following grounds:

State trial conflicts,

IT IS ORDERED vacating the Trial setting of 02/23/2017 and resetting same to **06/05/2017 at 8:00 a.m.** before the Master Calendar Assignment Judge.

IT IS ORDERED vacating the Final Trial Management Conference set this date and resetting same to **05/25/2017 at 8:30 a.m.** before this division.

IT IS ORDERED setting Status Conference on **03/30/2017 at 8:30 a.m.** before this division.

The Defendant having waived the applicable time limits,

IT IS ORDERED excluding all time between 02/23/2017 and 06/05/2017 (102 days).
NEW LAST DAY: 06/25/2017.

IT IS ORDERED affirming prior custody orders.

Pursuant to the Ruling entered, and there being no further need to retain the exhibits not offered in evidence in the custody of the Clerk of the Court,

IT IS ORDERED that the Clerk permanently release all exhibits not offered in evidence to the counsel/party causing them to be marked or written designee. Counsel/party or written

SUPERIOR COURT OF ARIZONA
MARICOPA COUNTY

CR2015-005499-001 DT
CR2015-119746-001 DT

02/17/2017

designee shall have the right to refile relevant exhibits as needed in support of any appeal or post-conviction relief. Refiled exhibits must be accompanied by a Notice of Refiling Exhibits and presented to the Exhibits Room of the Clerk's Office. The Court's exhibit tag must remain intact on all refiled exhibits.

IT IS FURTHER ORDERED that counsel/party or written designee take immediate possession of all exhibits referenced above.

ISSUED: Exhibit Release Form

FILED: Exhibit worksheet

2:46 p.m. Matter concludes.

WILLIAM G MONTGOMERY
MARICOPA COUNTY ATTORNEY

Erin M Pedicone
Deputy County Attorney
Bar ID #: 029094
301 W. Jefferson, 5th Floor
Phoenix, AZ 85003
Telephone: (602) 506-8556
mcaosvd@mcao.maricopa.gov
MCAO Firm #: 00032000
Attorney for Plaintiff

IN THE SUPERIOR COURT OF THE STATE OF ARIZONA

IN AND FOR THE COUNTY OF MARICOPA

THE STATE OF ARIZONA,

Plaintiff,

vs.

THOMAS TOLWORTHY,

Defendant.

CR2015-005499-001

CR2015-119746-001

STATE'S MOTION AND ORDER TO
DISMISS WITHOUT PREJUDICE


(Assigned to the Honorable Mark
Brain)

The State of Arizona, pursuant to Rule 16.6, Arizona Rules of Criminal Procedure, moves to dismiss CR2015-119746-001 and CR2015-005499-001 without prejudice as to THOMAS TOLWORTHY because dismissal is in the interests of justice.

This Motion is not for the purpose of avoiding Rule 8, Arizona Rules of Criminal Procedure.

Submitted April 2, 2018.

WILLIAM G MONTGOMERY
MARICOPA COUNTY ATTORNEY

BY: 
/s/ Erin M Pedicone
Deputy County Attorney

Copy delivered
April 2, 2018, to:

The Honorable Mark Brain
Judge of the Superior Court

Philip O. Beatty
Attorney for Defendant

BY: 
/s/ Erin M Pedicone
Deputy County Attorney

emp

WILLIAM G MONTGOMERY
MARICOPA COUNTY ATTORNEY

Erin M Pedicone
Deputy County Attorney
Bar ID #: 029094
301 W. Jefferson, 5th Floor
Phoenix, AZ 85003
Telephone: (602) 506-8556
mcaosvd@mcao.maricopa.gov
MCAO Firm #: 00032000
Attorney for Plaintiff

IN THE SUPERIOR COURT OF THE STATE OF ARIZONA

IN AND FOR THE COUNTY OF MARICOPA

THE STATE OF ARIZONA,

Plaintiff,

vs.

THOMAS TOLWORTHY ,

Defendant.

CR2015-119746-001
CR2015-005499-001

ORDER

Upon Motion by the State of Arizona, it is ordered dismissing CR2015-119746-001 and CR2015-005499-001 against THOMAS TOLWORTHY without prejudice.

Dated April ____, 2018.

The Honorable Mark Brain
Judge of the Superior Court

FILED

2015 JUN 17 PM 1:45

CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
SANTA ANA

BY _____

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
SOUTHERN DIVISION

September 2014 Grand Jury

SACR15-00063

UNITED STATES OF AMERICA,
Plaintiff,
v.
TODD CHRISTIAN HARTMAN,
Defendant.

No. SA CR

I N D I C T M E N T

[18 U.S.C. §§ 2252A(a)(2),
(b)(1): Distribution of Child
Pornography; 18 U.S.C.
§§ 2252A(a)(5)(B), (b)(2):
Possession of Child
Pornography]

The Grand Jury charges:

COUNT ONE

[18 U.S.C. §§ 2252A(a)(2), (b)(1)]

On or about October 16, 2014, in Orange County, within the
Central District of California, defendant TODD CHRISTIAN HARTMAN
knowingly distributed at least one image of child pornography
and material containing child pornography, as defined in Title
18, United States Code, Section 2256(8)(A), namely, a video
titled "(-pthc center-)(opva)(2013) Cumming over loli_s pussy

1 2010 7yo_and_Dad BRILLIANT.wmv" that had been mailed, and
2 shipped and transported using any means or facility of
3 interstate and foreign commerce, and in and affecting interstate
4 and foreign commerce by any means, including by computer,
5 knowing that the video was child pornography.

6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

COUNT TWO

[18 U.S.C. §§ 2252A(a)(2), (b)(1)]

From on or about December 29, 2014, to on or about December 30, 2014, in Orange County, within the Central District of California, defendant TODD CHRISTIAN HARTMAN knowingly distributed at least one image of child pornography and material containing child pornography, as defined in Title 18, United States Code, Section 2256(8)(A), namely, a video titled "Kidcam - Mirey-12Y (2010)Pthc!!avi" that had been mailed, and shipped and transported using any means or facility of interstate and foreign commerce, and in and affecting interstate and foreign commerce by any means, including by computer, knowing that the video was child pornography.

COUNT THREE

[18 U.S.C. §§ 2252A(a)(5)(B), (b)(2)]

On or about February 5, 2015, in Orange County, within the Central District of California, defendant TODD CHRISTIAN HARTMAN knowingly possessed an HP Pavilion a1640n Computer Tower, bearing serial number CNH6441569, that contained at least one image of child pornography, as defined in Title 18, United States Code, Section 2256(8)(A), that had been mailed, shipped and transported using any means and facility of interstate and foreign commerce and in and affecting interstate and foreign commerce by any means, including by computer, and that was produced using materials that had been mailed, and shipped and transported in and affecting interstate and foreign commerce by

///

///

///

1 any means, including by computer, knowing that the image was
2 child pornography.

3 A TRUE BILL

4
5 Foreperson

6 STEPHANIE YONEKURA
7 Acting United States Attorney

8 
9 ROBERT E. DUGDALE
10 Assistant United States Attorney
11 Chief, Criminal Division

12 DENNISE D. WILLETT
13 Assistant United States Attorney
14 Chief, Santa Ana Office

15 JOSEPH T. MCNALLY
16 Assistant United States Attorney
17 Deputy Chief, Santa Ana Office

18 IVY A. WANG
19 Assistant United States Attorney
20 Santa Ana Office

1 EILEEN M. DECKER
 United States Attorney
 2 DENNISE D. WILLETT
 Assistant United States Attorney
 3 Chief, Santa Ana Branch Office
 ANNE C. GANNON (Cal. Bar No. 214198)
 4 Assistant United States Attorney
 United States Courthouse
 5 411 West Fourth Street
 Santa Ana, California 92627
 6 Telephone: (714) 338-3548
 Facsimile: (714) 338-3561
 7 E-mail: anne.gannon@usdoj.gov

8 Attorneys for Respondent
 UNITED STATES OF AMERICA

9 UNITED STATES DISTRICT COURT

10 FOR THE CENTRAL DISTRICT OF CALIFORNIA

11 UNITED STATES OF AMERICA,

12 Plaintiff,

13 v.

14 TODD CHRISTIAN HARTMAN,

15 Defendant.

No. SA CR 15-63(A)-JLS

GOVERNMENT'S OPPOSITION TO
DEFENDANT'S MOTION TO COMPEL
DISCOVERY

MOTION HEARING: 10/16/2015
 11:00 a.m.
 ESTIMATE: 20 minutes

17 The government files its opposition to defendant's motion to
 18 compel discovery pursuant to Federal Rule of Criminal Procedure 16.

19 Dated: September 24, 2015

Respectfully submitted,

20 EILEEN M. DECKER
 United States Attorney

21 DENNISE D. WILLETT
 Assistant United States Attorney
 Chief, Santa Ana Branch Office

22 /s/
 23 _____
 ANNE C. GANNON
 Assistant United States Attorney

24 Attorneys for Respondent
 UNITED STATES OF AMERICA

1 MEMORANDUM OF POINTS AND AUTHORITIES

2 I. INTRODUCTION

3 Law enforcement agencies have designed various technologies and
4 software to aid in their investigations of child pornography
5 possession and trafficking offenses. Peer Spectre is one such
6 investigatory tool. For the most part, technologies like Peer
7 Spectre are designed to function like publicly-available, share-file
8 programs that child pornography perpetrators use to commit their
9 crimes. However, the law enforcement software has been tailored to
10 provide specific information about perpetrators that can be used to
11 identify and apprehend them.

12 On September 18, 2015, defendant Todd Christian Hartman
13 ("defendant") filed a motion to compel extensive discovery relating
14 to Peer Spectre, including its specifications and a copy of the
15 software itself (the "requested information"). Defendant contends
16 that Peer Spectre was used to download images from defendant's
17 computer that formed the basis for the search warrant affidavit and
18 search of defendant's home. (Def. Mot. at 3.)¹ As described below,
19 defendant's motion should be denied because A) the requested
20 materials are protected by a qualified law enforcement privilege;
21 B) he has not established that the requested information is material
22 to his defense; and C) his request is overbroad.

23
24
25 ¹ While Peer Spectre was used in this investigation, it served a
26 different function. Peer Spectre reads publically available
27 information about which Internet Protocol ("IP") addresses are
28 offering child sexual abuse images online. A different program,
Shareaza LE, is used to actually download the publicly available
images and videos from a single user once Peer Spectre identifies the
IP address.

1 **II. STATEMENT OF FACTS**

2 Defendant is charged with one count of possession of child
3 pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B), and two
4 counts of transportation of child pornography, in violation of 18
5 U.S.C. § 2252A(a)(1). The transportation of child pornography counts
6 are based on Newport Beach Police Department Detective David Syvock
7 downloading child pornography videos from an Internet Protocol
8 address that resolved back to defendant's residence.

9 The government has produced materials relating to defendant's
10 case during the course of discovery, including a description in the
11 search warrant affidavit of how Peer Spectre works and Detective
12 Syvock's reports. In addition, the government recently disclosed 63
13 digital files related to the downloading of the charged videos via
14 the Shareaza LE program..

15 On September 9, 2015, defendant requested the following
16 materials, which are the subject of the instant motion to compel:

- 17 1. An installable copy of the Peer Spectre program used by
18 Detective David Syvock of the Newport Beach Police
19 Department, as described in his Affidavit in Support of
20 Search Warrant dated February 3, 2015. If difference
versions of the program exist, please provide a copy of
the version used by Detective Syvock during his
investigation of [defendant].
- 21 2. All documents in the government's possession, custody, or
22 control - and in the possession, custody, or control of
23 other law enforcement agencies involved with this
24 investigation, including the Newport Beach Police
Department - regarding Peer Spectre, including documents
regarding the program's technical specifications.
- 25 3. All documents and records in the government's possession,
26 custody or control - and in the possession, custody or
27 control of other law enforcement agencies involved in
28 this investigation, including the Newport Beach Police
Department - regarding any other software, computer
programs, or the like, used by Detective Syvock during
this investigation of [defendant].

1 (Def.'s Mot. at Ex. A.) The government responded to defendant's
2 request on September 16, 2015. (Def.'s Mot. at Ex. B.)

3 **III. ARGUMENT**

4 Defendant is not entitled to the requested materials because
5 A) the requested materials are protected by a qualified law
6 enforcement privilege; B) he has not established that the requested
7 information is material to his defense; and C) his request is
8 overbroad. The government has complied, and will continue to comply,
9 with its discovery obligations and defendant's motion should be
10 denied.

11 **A. PEER SPECTRE IS A SENSITIVE LAW ENFORCEMENT INVESTIGATORY**
12 **TOOL PROTECTED BY A QUALIFIED PRIVILEGE**

13 Sensitive, investigatory techniques should not be subject to
14 discovery without a showing of particular need.² In this regard,
15 courts have long recognized a qualified law enforcement privilege.³

16 The Supreme Court first recognized a qualified law enforcement
17 privilege in the context of the government's ability to withhold the
18 identity of informants. Roviaro v. United States, 353 U.S. 53
19 (1957). Numerous circuits have extended Roviaro to other sensitive
20 law enforcement investigative techniques, particularly relating to
21 electronic surveillance. In United States v. Van Horn, the Eleventh
22 Circuit outlined the rationale for such an expansion of the qualified
23 law enforcement privilege:

24 Disclosing the precise locations where surveillance devices
25 are hidden or their precise specifications will educate
criminals regarding how to protect themselves against

26 ² The standard for showing a particular need is addressed in
Part II.B. below.

27 ³ Claims of privilege are governed by common law. Fed. R. Evid.
28 501.

1 police surveillance. Electronic surveillance is an
2 important tool of law enforcement, and its effectiveness
3 should not be unnecessarily compromised. Disclosure of such
information will also educate persons on how to employ such
techniques themselves

4 789 F.2d 1492, 1508 (1986). See also United States v. Green,
5 670 F.2d 1148, 1155 (D.C. Cir. 1981) (“[P]olicy justifications
6 analogous to those underlying the well-established informer's
7 privilege support a qualified privilege protecting police
8 surveillance locations from disclosure.”); United States v.
9 Crumley, 565 F.2d 945, 950 (5th Cir. 1978) (holding that the
10 government need not disclose the location of “track sheets”
11 [computer printouts listing all parts, including identification
12 numbers, used in the assemblage of a vehicle] because “they are
13 valuable tools used by law enforcement officers in discovering
14 and solving motor vehicle thefts”); accord United States v.
15 Cintolo, 818 F.2d 980 (1st Cir. 1987) (upholding limitations the
16 district court placed on defendant’s cross-examination of agent
17 regarding electronic surveillance techniques); United States v.
18 Gazie, 786 F.2d 1166, at *8 (6th Cir. 1986) (limiting cross-
19 examination regarding the type and location of electronic
20 microphone surveillance, despite defendant’s desire to use the
21 information to claim the voices were distorted).

22 Courts within the Ninth Circuit have also applied Roviaro to
23 other sensitive law enforcement investigative techniques. See United
24 States v. Rigmaiden, 844 F. Supp. 2d 982, 999 (D. Ariz. 2012)
25 (holding that “real time and historical geolocation techniques” and
26 “radio wave collection methods” used by the government were “subject
27 to the Roviaro privilege” because disclosure “would hamper future law
28

1 enforcement efforts by enabling adversaries of law enforcement to
2 evade detection"); see also United States v. Diaz, No. 2:13-CR-00148-
3 JAD, 2014 WL 1668600, at *2-*3 (D. Nev. Apr. 25, 2014) (noting that
4 "[p]ersuasive authority from other circuits has extended Rovario to
5 recognize 'a qualified government privilege not to disclose sensitive
6 investigative techniques,' provided the exclusion of such techniques
7 does not unduly prejudice the defense" and therefore granting the
8 government's motion in limine to preclude questioning regarding the
9 specifics of a recording device) (quoting Van Horn, 789 F.2d at
10 1507). Cf. United States v. Budziak, 697 F.3d 1105, 1113 (9th Cir.
11 2012) (recognizing that "law enforcement confidentiality concerns"
12 may play a role in disclosure on remand); United States v. Mahon, No.
13 CR09-0712 PHX-DGC, 2011 WL 5006737, at *5 (D. Ariz. Oct. 20, 2011)
14 (stating that because "[c]ourts have applied the Rovario qualified
15 privilege to the location and composition of electronic surveillance
16 information," if "disclosure of [wireless transmitter, electret
17 microphone, and wireless receivers] would compromise sensitive law
18 enforcement information," the court would engage in a Rovario
19 analysis).

20 The qualified law enforcement privilege has been applied
21 specifically to child pornography cases. In United States v.
22 Pirosko, the defendant sought to compel investigative software
23 similar to Peer Spectre. See 787 F.3d 358, 363-64 (6th Cir. 2015).
24 The Sixth Circuit found persuasive the government's argument that
25 granting the motion to compel "would compromise the integrity of its
26 surveillance system and would frustrate future surveillance efforts"
27 and, therefore, upheld denial of the motion. See id. at 365-67.

1 Further, in United States v. Chiaradio, the First Circuit recognized
2 that "the source code [for EP2P, an FBI investigatory tool for child
3 pornography cases,] is purposely kept secret because the government
4 reasonably fears that traders of child pornography (a notoriously
5 computer-literate group) otherwise would be able to use the source
6 code to develop ways either to evade apprehension or to mislead the
7 authorities." 684 F.3d 265, 278 (2012).

8 The confidentiality concerns in this case are the same as those
9 expressed in Pirosko, Chiaradio, and the many other surveillance
10 technology privilege cases cited above. Permitting disclosure of a
11 copy of Peer Spectre or its specifications, and similar software,
12 would give defendant an insider's perspective of how the software
13 works, thereby educating him (and other child pornography
14 perpetrators) on how to avoid detection by Peer Spectre in the
15 future. As Chiaradio notes, child pornography perpetrators are "a
16 notoriously computer-literate group." 684 F.3d at 278. Indeed, this
17 fact makes the concerns of disclosing technology specifications even
18 higher in child pornography cases than in cases of video and
19 microphone surveillance, such as Van Horn, where the qualified law
20 enforcement privilege has also been upheld.

21 **B. DEFENDANT HAS NOT ESTABLISHED THAT THE REQUESTED**
22 **INFORMATION IS MATERIAL TO HIS DEFENSE**

23 Because a qualified law enforcement privilege exists for the
24 requested information, "[t]he burden of proof is on the defendant[]
25 to show need for the disclosure." United States v. Sai Keung Wong,
26 886 F.2d 252, 256 (9th Cir. 1989). The defendant must first make a
27 threshold showing of materiality, based on more than "speculation" or
28 "suspicion," that the disclosure would be relevant to his case. See

1 United States v. Ibarra, 581 F. Appx. 687, 689 (9th Cir. 2014). As
2 the Ninth Circuit noted in United States v. Budziak, "conclusory
3 allegations of materiality [will not] suffice.'" 697 F.3d 1105, 1111
4 (9th Cir. 2012) (quoting United States v. Mandel, 914 F.2d 1215, 1219
5 (9th Cir. 1990)).⁴

6 If the defendant fails to make this threshold showing of
7 materiality, the motion to compel must be denied. See Ibarra, 581 F.
8 Appx. at 689 (upholding the district court's denial of defendant's
9 motion for in camera review of an informant's file or to disclose the
10 identity of the informant because the defendant "provided only
11 speculation and suspicion" that the information "would be 'relevant'
12 or 'helpful' to any defense"). Only when the defendant has made this
13 threshold showing of materiality should the court proceed to "balance
14 1) the extent to which disclosure would be relevant and helpful to
15 the defendant's case, and 2) the government's interest in protecting"
16 the sensitive information. United States v. Spires, 3 F.3d 1234,
17 1238 (9th Cir. 1993); see also Roviaro, 353 U.S. at 62 (noting that
18 the court must consider "the public interest in protecting the flow
19 of information against the individual's right to prepare his
20 defense"). If the threshold showing is made, an ex parte, in camera
21 hearing of the requested information will be held to aid the court in
22

23 ⁴ Here, the standard for materiality is the same as in Federal
24 Rule of Criminal Procedure 16. Compare United States v. Ibarra, 581
25 F. Appx. 687, 689 (9th Cir. 2014) (stating the standard for threshold
26 materiality in the law enforcement privilege context as whether the
27 discovery "would be 'relevant' or 'helpful' to any defense), with
28 United States v. Doe, 705 F.3d 1134, 1151 (9th Cir. 2013) (stating
the standard for Rule 16 materiality as whether the discovery "would
. . . have been helpful to [the] defense"). Therefore, if defendant
has not met the qualified law enforcement privilege threshold for
materiality, he also has not met the Rule 16 standard.

1 balancing the parties' interests. United States v. Salazar, 598 F.
2 Appx. 490, 493 (9th Cir. 2015).

3 First, defendant has not made the requisite threshold showing of
4 materiality. Defendant mistakenly relies on United States v.
5 Budziak to support his claim of materiality. (Def.'s Mot. at 5-6.)
6 In Budziak, the court held that discovery of law enforcement software
7 was material to his defense when the defendant's motions to compel
8 had included evidence "suggesting that the FBI may have only
9 downloaded fragments of child pornography files[,] . . . making it
10 'more likely' that he did not knowingly distribute any complete child
11 pornography files." 697 F.3d at 1112. The defendant also "submitted
12 evidence suggesting that the FBI agents could have used the . . .
13 software to override his sharing settings." Id. Indeed, the
14 defendant presented testimony of a computer forensics expert stating
15 what additional information could be uncovered through inspection of
16 the software and be helpful to his defense. Id. The Budziak court
17 noted that unlike in Chiaradio, where "the defendant 'neither
18 contradicted nor cast the slightest doubt upon' the government's
19 testimony [regarding] the materials it had already provided to him[,]
20 . . . Budzik presented arguments and evidence suggesting that the
21 materials disclosed by the FBI did not resolve all questions relevant
22 to his defense." Id. at 1112 n.1 (quoting Chiaradio, 684 F.3d at
23 277) (emphasis added). Because the evidence submitted by the Budziak
24 defendant demonstrated precisely how the requested information would
25 be helpful to his specific defenses, the court held the discovery
26 material. Id. at 1112-13.

27 This case is like Chiaradio, not Budziak. Defendant makes two
28

1 "conclusory allegations of materiality" for the requested
2 information: that whether he "knowingly shared child pornography
3 hinges on the technical specifications and reliability of this
4 computer program;" and that information regarding "how Peer Spectre
5 works and its reliability" is necessary for cross-examining Detective
6 Syvock. (Def.'s Mot. at 5.) Here, defendant fails to provide any
7 detail as to how Peer Spectre's technical specifications could help a
8 specific defense. Whereas the Budziak defendant "identified specific
9 defenses to the distribution charge that discovery on the [law
10 enforcement] program could potentially help him develop," 697 F.3d at
11 1112, defendant can offer no explanation for how the requested
12 information could rebut his distribution charges. See also Pirosko,
13 787 F.3d at 365 (distinguishing Budziak on the fact that the Budziak
14 defendant had "presented evidence," including expert testimony, of
15 how the discovery would help two specific defense claims and noting
16 that "it is important for the defendant to produce some evidence of
17 government wrongdoing").

18 Just as in Budziak, the government has provided defendant with a
19 description of how Peer Spectre works. In Budziak, however, the
20 defendant's charge was "predicated largely on computer software
21 functioning in the manner described by the government." 697 F.3d at
22 1113. That is not precisely the case here. The government's case is
23 also based on the same files being found on defendant's computer
24 after it had been seized. Because defendant's case is distinct from
25 Budziak in this significant regard, defendant cannot present the
26 types of evidence regarding his need for the information that were
27 persuasive to the Budziak court.

28

1 Even if defendant could satisfy the requisite threshold showing
2 of materiality, he would not be entitled to the requested
3 information. The public interests in limiting disclosure of Peer
4 Spectre's specification information are vast, as outlined in Part
5 III.A. above, and outweigh any relevance defendant could allege to
6 his case.⁵

7 **C. DEFENDANT'S REQUEST IS OVERBROAD**

8 Defendant requests "[a]ll documents . . . regarding Peer
9 Spectre." Defendant does not attempt to describe the types of
10 information or documents sought regarding Peer Spectre, nor does he
11 limit the request to documents regarding his case. It would be
12 incredibly burdensome for the government to gather every document it
13 has regarding Peer Spectre, not to mention the immateriality and
14 confidentiality concerns that would arise with respect to Peer
15 Spectre documents for other defendants. Because defendant's request
16 is unreasonable and overbroad, his motion should be denied.

17 **IV. CONCLUSION**

18 For the foregoing reasons, defendant's motion to compel should
19 be denied.

20
21
22
23
24
25 ⁵ Because defendant has provided no indication of how the
26 requested information is material to his defense, the government
27 cannot presently make a specific argument regarding the balancing of
28 interests required by Roviaro and Spires. The government reserves
the right to supplement this argument.

*** The Child Protection System (CPS) - Acceptable Use Requirements ***

By using this tool you acknowledge and agree to:

I understand all software utilizing to The Child Protection System (CPS) requires a license. Licenses are issued to individual investigators and can only be used by the license holder unless otherwise authorized by the intellectual property owner. Where software is restricted to law enforcement agency use, users must discontinue use of the system if they are no longer in good standing with their law enforcement agency. Individuals who change agencies must obtain a new license so as to preserve historic or transactional data.

I am the authorized user associated with this license and am in good standing with my law enforcement agency. I am authorized by my agency to investigate or assist in the investigation of child exploitation crimes.

This software supports active law enforcement investigations; therefore no persons shall publicly demonstrate this system or the software provided without the expressed permission of the software owner. Users who expose data obtained through this system to non-law enforcement without expressed permission may have their licenses suspended.

Users of the provided software shall not reverse engineer or in any other way attempt to circumvent the intellectual property rights of the software owner or server provider. Those using the software must conform to the license and use agreements established by the owners of both client and server applications.

I understand that records related to peer-to-peer investigations are stored on servers belonging to a credentialed law enforcement entity. I understand that other participating law enforcement agencies may have need to access that data where it is appropriate and related to their investigations. I understand that this information will remain permanently available to all related agencies, even if I cease to use the system or withdraw in any way from law enforcement.

Users of this system are required to deconflict their investigations. If you use the query system to identify offenders you are free to conduct your investigation in the manner supported by your agency but you are required to log your investigative interest in the given IP, moniker, etc. using the provided tools. You shall not use this system in conjunction with investigations that initiate investigations outside of your jurisdiction unless you have received a previous agreement from the corresponding jurisdiction (This does not apply to situations where the investigative lead appeared to originate in your jurisdiction but was later determined to be elsewhere).

No user of the system may sell or otherwise profit from the use of the CPS, the resulting leads, or related software without the expressed permission of the intellectual property owner. Approved tools that are offered for distribution must be free to law enforcement, authorized to work the related investigations. Additionally, all training materials developed for tools offered for distribution must be made available to all users of the related software without cost for use or distribution. This information is law enforcement sensitive.

With the exception of peer-to-peer locate information, all data must be verified with the appropriate source agency prior to any law enforcement action.

Shared data may be segregated as needed to maintain operational security. System activity is logged on law enforcement servers only. Communications with other servers from these applications is not logged.

Use of this system, the software and the related data and features is a privilege and may be revoked at any time.

Additional guidelines and requirements will be added as the situation warrants.

Unconfirmed Subscriber Data provided by TLO is unconfirmed. It originates from a variety of sources and is subject to omission, alteration or misrepresentation. Do not use this data for probable cause. It must be confirmed through other investigative means that are acceptable with your agency and prosecuting attorney. TLO provides no warranty or guarantee of any kind regarding data provided free to law enforcement and assumes no responsibility for the use of software or resulting information. You agree to indemnify, defend and hold harmless TLO and its suppliers from any and all claims arising from or relating to your use of the software or data obtained from TLO. Commercially reasonable efforts will be made to keep these servers available and the resulting services shall remain perpetually free to law enforcement engaged in child exploitation investigations.

Failure to follow any of these conditions may result in the suspension or revocation of your license.

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
SOUTHERN DIVISION**

UNITED STATES OF AMERICA,

Plaintiff,

v.

TODD CHRISTIAN HARTMAN,

Defendant.

Case No. CR 15 00063

AFFIDAVIT OF TAMI LOEHRS

I, TAMI L. LOEHRS, hereby declare as follows:

1. I am a computer forensics expert and owner of Loehrs& Associates, LLC (formerly Law2000, Inc.) a firm specializing in computer forensics. My offices are located at 3037 West Ina, Suite 121, Tucson, Arizona 85741. I am competent to testify and the matters contained herein are based on my own personal knowledge.

2. I have been working with computer technology for over 20 years and I hold a Bachelor of Science in Information Systems. I have completed hundreds of hours of forensics training including courses with Guidance Software and Access Data. I am an EnCase Certified Examiner (EnCE), an Access Data Certified Examiner (ACE), a Certified Computer Forensic Examiner (CCFE) and a Certified Hacking Forensic Investigator (CHFI). I have conducted hundreds of forensics exams on thousands of pieces of evidence including hard drives, cell phones, removable storage media and other electronic devices. I have conducted seminars on Computer Forensics and Electronic Discovery throughout the United States. In addition, I hold a Private Investigator Agency License in the State of Arizona which requires a minimum of

6,000 hours investigative experience. My Curriculum Vitae is attached hereto and updated versions may be downloaded from the Loehrs & Associates website at www.ForensicsExpert.net.

3. I have been the computer forensics expert for the defense on over 250 child pornography cases throughout the United States, Puerto Rico, Marianna Islands, Canada and England since the year 2000 and have testified over ninety times in State, Federal and international Courts.

4. I have been retained as a computer forensics expert by Cuauhtémoc Ortega, Deputy Federal Public Defender and counsel for Defendant Todd Christian Hartman, for the purpose of assisting with matters related to the searching, collecting, analyzing and producing of electronic evidence in this matter.

5. I have reviewed discovery materials produced by the government including, but not limited to, Newport Beach Police Department Reports (Bates 007-0010), Search Warrant and Affidavit prepared by Detective David Syvock (Bates 0045-0066), Department of Homeland Security Report of Investigation (Bates 0023-0032), the Indictment and Superseding Indictment, and Defense Motion to Compel dated September 18, 2015.

6. According to the Affidavit prepared by Detective Syvock, this case originated from an undercover investigation of the peer-to-peer network known as eDonkey2000. On October 16, 2014, Det. Syvock identified files of suspect child pornography as “available for sharing” from a computer with a specific GUID at the IP address 76.172.3.11. He does not indicate what software or tools he used to identify the files of child pornography. Det. Syvock indicates he downloaded five (5) files on October 16th and provides information about those files on pages 13 through 15. Although two of the files provided indicate they were downloaded on

10/16/2014, the other three files have dates nearly one month later on 11/06/2014 and 11/11/2014. Det. Syvock does not indicate what software or tools he used to download those files.

7. On November 23, 2014, Det. Syvock identified files of suspect child pornography as “available for sharing” on a computer with the same GUID but with a different IP address of 76.171.211.243. Again, he indicates he downloaded one (1) file and includes that information on page 16. However, the file is dated over one month later on 12/29/2014. Again, he makes no mention of the software or tools used to conduct his investigation.

8. Although Det. Syvock does not specifically identify the software or tools he used during his undercover investigation, he makes general references in his affidavit to the Child Protection System (CPS) and Peer Spectre.

9. I know from experience on numerous P2P cases and from personally listening to the testimony of law enforcement personnel, including William Wiltse, that CPS was created at Wiltse’s direction. Wiltse is or was the Director of Software Programming at TLO, a data fusion company in Boca Raton that, among other things, develops software to assist law enforcement who are investigating child exploitation crimes. CPS is a proprietary suite of software tools created by and used exclusively by law enforcement that includes *Peer Spectre 2* and its predecessor *Peer Spectre*. CPS has been used by law enforcement in numerous cases throughout the country in which I have been involved as a defense expert including the matters of *United States vs. Angel Ocasio, EP-11-CR-2728(KC)* and *United States vs. John A. Crowe, 11CR 1690*. These cases, as well as others, have brought to light serious concerns with regard to the CPS software and whether that software is going beyond the scope of “publicly available” information. To my knowledge, as of the writing of this Affidavit, this software has never been

formally tested and/or validated by anyone and is unavailable for testing by any third-parties. Although the courts in *Crowe* and *Ocasio* agreed to third-party testing of the software, both cases were settled and the software was never made available to me.

12. It is critical to Mr. Hartman's defense to understand how this software functions in order to determine its reliability and accuracy in identifying files reported as "publicly available" from Mr. Hartman's computer.

13. On September 30, 2015, an independent forensics examination was conducted on the evidence seized from Mr. Hartman's residence, specifically a Hewlett Packard Pavilion desktop computer (HP Pavilion). During that examination, a search for the six files downloaded during the undercover investigation revealed all six files were located on Hartman's computer in a folder with over 4,000 files associated with the eMule software application.

14. eMule is a P2P file sharing software application that shares information through the eDonkey network. eMule was installed on the HP Pavilion in March of 2014 but uninstalled before the execution of the search warrant. A review of the eMule system files revealed only 600 files were "publicly available" for sharing even though over 4,000 files existed in the eMule default folders. Four (4) of the files identified during the undercover investigation were not included in this list of "publicly available" files. The remaining two (2) files identified during the undercover investigation were found to be "publicly available" but had not been shared since May, 2014, nearly three months prior to the undercover investigation. This begs the question of how the CPS software identified the files in the first place if they are not listed as "publicly available" from Hartman's computer.

15. Additionally, the software PeerBlock was installed on the HP Pavilion in December of 2013. Peer Block functions as a firewall that blocks IP addresses manually entered into the software or IP addresses that have been included in “blacklists” available online. A review of the system files for this application revealed the user enabled to block IP addresses associated with peer to peer file sharing.

16. Thus, the implication in this case is that the CPS software may be identifying files of suspect child pornography on Hartman’s computer that are not “publicly available” and were not intended to be shared.

17. For all of the reasons stated above, and under general scientific principles, it is my opinion that there is insufficient forensic evidence to corroborate that files of suspect child pornography identified during the undercover investigation were “publicly available”. In addition, it remains my opinion that law enforcement’s proprietary CPS software needs to be tested by a qualified third-party to determine its functionality and accuracy.

18. I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Dated: October 8, 2015



Tami L. Loehrs

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
27
28

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,
Plaintiff,
v.
TODD CHRISTIAN HARTMAN,
Defendant.

Case No. SACR 15-00063-JLS
**ORDER RE PRETRIAL
MOTIONS**

Defendant is charged with two counts of transportation of child pornography in violation of 18 U.S.C. § 2252A(a)(1) and one count of possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). Trial is currently set for December 1, 2015, and currently before the Court are a number of pretrial motions, which have been fully briefed and argued.¹ Specifically, presently before the Court are (1) the Government’s Motion in Limine [No. 1] to Admit Child Pornography Images and Videos (Docs. 18, 25, & 38); (2) Defendant’s Motion to Suppress Evidence² (Docs. 26, 35, 49, 69 & 76); (3) Defendant’s Motion to Compel Discovery

¹ The motions were heard on October 16, 2015, and October 27-28, 2015. (*See* Docs. 55 & 61-62.) Evidence was admitted as to Defendant’s Motion to Compel Discovery and to Suppress Evidence. The Court authorized the filing of post-hearing briefs as to the Motion to Compel Discovery and Motion to Suppress. In connection with its ruling on the present Motions, the Court has reviewed and considered the parties’ filings, their argument, and the admitted evidence.
² For the first time after the hearing, Defendant suggests that a challenge to the validity of the warrant may be forthcoming. (Def.’s Post-Hr’g Brief at 3 n.3.) That issue is not currently before the

1 (Docs. 27, 37, 47, 50 & 68-69); (4) Defendant’s Motion in Limine [No. 1] to Exclude
2 “Other Acts” Evidence (Docs. 28, 40 & 48); and (5) Defendant’s Motion to Exclude
3 Expert Testimony (Docs. 51-52).

4 A discussion of the Court’s rulings as to all pretrial Motions is set forth below.

5 **I. GOVERNMENT’S MOTION *IN LIMINE* TO ADMIT CHILD**
6 **PORNOGRAPHY VIDEOS AND IMAGES**

7 The Government filed a Motion *in Limine* to Admit Child Pornography Images
8 and Videos. (Doc. 18.) Defendant Todd Christian Hartman filed a timely Opposition
9 brief, and the Government filed a Reply brief. (Docs. 25 & 38.) As set forth below, the
10 Court GRANTS IN PART the Government’s Motion.

11 **A. Evidence at Issue**

12 The Government moves to admit approximately ten videos and twenty still
13 images³ that it contends meet the definition of child pornography.⁴ Defendant argues
14 that the probative value of such evidence is substantially outweighed by its unfair
15 prejudicial effect, and therefore the images should be excluded pursuant to Federal
16 Rule of Evidence 403.

17 **B. Elements of the Offense**

18 The First Superseding Indictment (“FSI”) charges Defendant with two counts of
19 transportation of child pornography (Counts 1 and 2) and one count of possession of
20 child pornography (Count 3). (Doc. 31.) To convict defendant of transportation of
21 child pornography, the Government must prove the following five elements beyond a
22 reasonable doubt:

23 Court, the Court has not considered it, and this Order does not address the validity of the search
24 warrant.

25 ³ Hereinafter, when discussing the Government’s present Motion in Limine, the Court’s references
26 to “the images” should be understood to refer to both videos and still images collectively.

27 ⁴ Six videos are identified in the Government’s Motion. (Mot. at 6-8.) Three others are identified in
28 the Reply. (Reply at 5.) Language in the Reply brief makes it unclear whether the Government still
intends to offer the twenty still images. (*See id.*)

The parties use the terms “child pornography” and “pornograph[y] . . . of minors,” which is defined
in 18 U.S.C. § 2256(8)(A), as meaning “any visual depiction, . . . of sexually explicit conduct, where
. . . the production of such visual depiction involves the use of a minor engaging in sexually explicit
conduct” *Id.*

1 First, that the defendant knowingly [transported] . . . a
2 visual depiction in interstate commerce by any means,
3 including a computer;

4 Second, that the production of such visual depiction
5 involved the use of a minor engaging in sexually explicit
6 conduct;

7 Third, that such visual depiction was of a minor
8 engaged in sexually explicit conduct;

9 Fourth, that the defendant knew that such visual
10 depiction was of sexually explicit conduct; and

11 Fifth, the defendant knew that at least one of the
12 persons engaged in sexually explicit conduct in such visual
13 depiction was a minor.

14 9th Cir. Crim. Jury Instr. 8.184 (2010). The charge of possession of child pornography
15 requires proof beyond a reasonable doubt of four similar elements:

16 First, that the defendant knowingly possessed [books]
17 [magazines] [periodicals] [films] [video tapes] [matters] that
18 the defendant knew contained [a] visual depiction[s] of [a]
19 minor[s] engaged in sexually explicit conduct;

20 Second, the defendant knew [each] [the] visual
21 depiction contained in the [[books] [magazines]
22 [periodicals] [films] [video tapes] [matters]] [[was of]
23 [showed]] [a] minor[s] engaged in sexually explicit conduct;

24 Third, the defendant knew that production of such [a]
25 visual depiction[s] involved use of a minor in sexually
26 explicit conduct; and

27 Fourth, that [each] [the] visual depiction had been
28 either

1 a) [mailed] [shipped] [transported] in interstate or
2 foreign commerce, or

3 b) produced using material that had been [mailed]
4 [shipped] [transported] in interstate or foreign commerce [by
5 computer [or other means]].

6 *Id.* at 8.185. “Sexually explicit conduct” is defined by statute as including “actual or
7 simulated . . . sexual intercourse, including genital-genital, oral-genital, anal-genital,
8 or oral-anal, whether between persons of the same or opposite sex; . . . masturbation[,]
9 . . . or [the] lascivious exhibition of the genitals or pubic area of any person” 18
10 U.S.C. § 2256(2)(A)(i), (iii) & (v).

11 C. The Parties’ Positions

12 The Government argues that the images are relevant to prove that Defendant
13 transported and possessed images that are in fact child pornography within the
14 statutory definition rather than merely innocent pictures of unclothed children. (Mot.
15 at 4.) Additionally, the Government contends that the images are relevant to prove
16 Defendant’s knowledge. (*Id.*) In response, Defendant argues that his willingness to
17 stipulate that the files at issue are “pornographic [depictions] of minors [that] depict
18 actual or ‘real’ children” obviates the Government’s need to introduce the images
19 themselves. (Opp’n at 2.) The Government counters that Defendant is unwilling to
20 stipulate to his knowledge that the images are sexually explicit depictions of minors
21 and that the persons depicted are minors. (Reply at 6.) Thus, in the Government’s
22 view, because Defendant is not willing to stipulate to all the elements that the images
23 are offered to prove, those images should be admitted. (*Id.*) Moreover, the
24 Government argues that it is entitled to present evidence of its choosing rather than
25 accepting a Defendant’s stipulation. (*Id.* at 3-5.)

26 D. Discussion

27 Both parties recognize that the evidence is to be excluded, if at all, pursuant to
28 Federal Rule of Evidence 403:

1 The court may exclude relevant evidence if its
2 probative value is substantially outweighed by a danger of
3 one or more of the following: unfair prejudice, confusing the
4 issues, misleading the jury, undue delay, wasting time, or
5 needlessly presenting cumulative evidence.

6 *Id.* Evidence is relevant if it has any tendency to make a fact of consequence “more or
7 less probable than it would be without the evidence.” Fed. R. Evid. 401.

8 Here, the relevance of the images to the elements of the charges is both obvious and
9 undeniable.

10 The images are highly probative of four of the five elements of the
11 transportation charges. Specifically, an examination of the content of the images will
12 likely influence the jury’s determination of whether the second and third elements are
13 met because it is highly likely to reveal whether there are depictions of any minors
14 engaged in sexually explicit conduct and whether actual minors engaging in sexually
15 explicit conduct were used in the production of the images. Moreover, examination of
16 the content of the images is highly likely to influence the jury’s determination of
17 whether a person viewing the content would, by simply viewing that content,
18 understand that the images constitute visual depictions of minors engaged in sexually
19 explicit conduct. Thus, the images are also highly probative of the fourth and fifth
20 elements of the transportation charges.

21 In the same manner, the images are highly likely to influence the jury’s
22 determination of three of the four elements of the possession charge. Like the
23 transportation charge, the images themselves are highly probative as to all elements of
24 the offense other than the transportation in commerce element.

25 Therefore, it is clear that the images are highly probative. However, the images
26 are also inherently inflammatory. Therefore, the Court must balance the probative
27 value against the danger of unfair prejudice before ruling on admissibility.

28 Defendant urges the Court to consider the availability of alternative evidence

1 and exclude the images themselves. Although Defendant has offered to stipulate that
2 the images fall into the definition of child pornography, this does not render those
3 images wholly excludable under Rule 403. As argued by the Government,
4 Defendant's stipulation does not address his knowledge of the content of the images in
5 the manner required to prove several of the elements of the charged offenses.

6 Defendant contends that in the Court's 403 analysis, the Court must factor in
7 his willingness to reach a stipulation with the Government regarding the content of the
8 files, relying on the Ninth Circuit case of *United States v. Merino-Balderrama*, 146
9 F.3d 758, 762 (9th Cir. 1998). (Opp'n at 2.) This case is distinguishable. In *Merino-*
10 *Balderrama*, the court held that the jury should not have been shown films of child
11 pornography where Defendant stipulated that the films contained child pornography
12 and that those films had traveled in interstate commerce. 146 F.3d at 761-63. As is the
13 case here, the defendant refused to stipulate to his knowledge of the content of the
14 films, and the films were shown to establish that knowledge. *Id.* The Ninth Circuit
15 found an abuse of discretion to show the films because the content of the films was
16 not probative of the defendant's knowledge because there was no evidence he had
17 viewed the films. *Id.* Rather, the boxes in which the film reels had been packaged,
18 which the defendant had seen, clearly depicted images of children (cut from the film)
19 engaged in sexual conduct. *Id.* In such an instance, the films themselves lacked any
20 additional probative value. *Id.*

21 Here, there is nothing analogous to the film reel boxes that is probative as to
22 Defendant's knowledge. This case involves intangible computer files rather than
23 tangible media, and therefore admission of images in this case can easily be limited to
24 images found in files where there is forensic evidence that Defendant actually
25 accessed. *Cf. United States v. Ganoë*, 538 F.3d 1117, 1124 (9th Cir. 2008) (“[F]or
26 every image shown to the jury there was forensic evidence that the files had actually
27 been opened and viewed after downloading.”).

28 The Court is not alone in rejecting Defendant's offer to stipulate as a means of

1 avoiding admission of child pornography images at trial. To the contrary, courts have
2 consistently admitted images of child pornography notwithstanding a defendant's
3 willingness to stipulate that the images at issue depict actual minors engaged in
4 sexually explicit conduct. *See, e.g., Ganoë*, 538 F.3d at 1123 (rejecting the argument
5 that the "probative value of the images was eliminated by his offer to stipulate that the
6 images represented actual children engaged in sexual conduct and that anyone seeing
7 the images even for a moment would know that they were child pornography");
8 *United States v. Cunningham*, 694 F.3d 372, 391 (3d Cir. 2012) (noting a "near-
9 uniform agreement that the admission of child pornography images or videos is
10 appropriate, even where the defendant has stipulated, or offered to stipulate, that those
11 images or videos contained child pornography" and collecting cases); *United States v.*
12 *Storm*, 915 F. Supp. 2d 1196, 1201 (D. Or. 2012) (collecting cases) *aff'd*, 612 F.
13 App'x 445 (9th Cir. 2015). Thus, Defendant's offer to stipulate to certain elements of
14 the charged offenses does not alter the admissibility of the images offered by the
15 Government.

16 Nevertheless, on the issue of unfair prejudice, the Court finds that it cannot
17 render a final decision in advance of trial regarding admissibility of all images sought
18 to be introduced at trial. As noted by Defendant, at some point, the law of diminishing
19 returns reduces the probative value of each additional image, and the danger of unfair
20 prejudice increases with each additional image to the point where that danger
21 substantially outweighs any incremental probative value of each additional image.
22 Relatedly, at some point, the presentation of additional images to the jury will amount
23 to the needless presentation of cumulative evidence, which also requires exclusion
24 pursuant to Rule 403.

25 However, that is not to say that the Court cannot make any pretrial rulings on
26 the issue of admissibility of the images. First, as a general rule, to the extent the
27 images are offered to show Defendant's knowledge, where the Government offers
28 evidence that Defendant actually opened and viewed the computer files at issue, the

1 Government may show the image to the jury. *Ganoe*, 538 F.3d at 1124. However, as
2 noted previously, at some point, even evidence of this type may cease to have
3 sufficient probative value, or may represent needlessly cumulative evidence, and the
4 Court will exclude it.

5 Second, as to the specific images offered, the Court declines Defendant's
6 invitation to limit the prosecution to showing the (presumably less inflammatory)
7 images that depict minors engaged in "sexually explicit conduct" that falls within the
8 § 2256(2)(A)(v) definition while excluding the (presumably more inflammatory)
9 images that fall within the definitions of § 2256(2)(A)(i) and (iii). The latter requires
10 depictions of acts of sexual intercourse (broadly defined), while the former requires
11 only "lascivious exhibition of the genitals or pubic area." 18 U.S.C. § 2256(2)(A)(i) &
12 (v). Defendant's point is that "videos showing oral sex or sexual intercourse are not
13 necessary." (Opp'n at 3.) However, a determination of whether the "exhibition of the
14 genitals or pubic area" is "lascivious" requires attention to subtle considerations that
15 are not implicated when the image at issue depicts actual or simulated sexual
16 intercourse (broadly defined). *See, e.g., United States v. Banks*, 556 F.3d 967, 979-80
17 (9th Cir. 2009) (noting that "applied to the conduct of children, lasciviousness is not a
18 characteristic of the child photographed but of the exhibition which the photographer
19 sets up for an audience that consists of himself or likeminded pedophiles.") (citation
20 omitted).

21 Third, and notably, the six videos intended to be offered by the Government are
22 described in its motion to total more than eighteen minutes in length. (Mot. at 6-8.)
23 Three more videos are described in the Reply, but the length of those videos are not
24 disclosed. (Reply at 5.) Taken together, these videos are far too lengthy, and are
25 highly prejudicial. Indeed, the length of any one of these videos exceeds the length
26 required to prove the elements of the charged offense to which it relates. The purpose
27 for which the videos are offered can be served by excerpts from those videos, or even
28 still images from those videos, and in unedited form, the Court is highly unlikely to

1 admit all these videos or to admit the entirety of any video. *Cf. Ganoë*, 538 F.3d at
2 1124-25 (“The district court limited the government to ten clips, each one lasting a
3 few seconds, with a total duration of under one minute.”).

4 **E. Ruling**

5 Subject to the discussion set forth above and articulated by the Court at the
6 October 16, 2015 Status Conference, the Court GRANTS IN PART the Government’s
7 Motion in Limine to Admit [No. 1] to Admit Child Pornography Images and Videos.

8 Thus, as articulated by the Court at the October 16, 2015 Status Conference, the
9 parties are directed to meet and confer regarding the images and videos to be offered
10 at trial. As represented by the Government at the Status Conference, its then-current
11 editing had reduced the length of 9 videos it intends to ask the Court to publish from
12 more than 18 minutes to approximately 4 minutes. (*See* 10/16/2015 Tr. at 5-6.) The
13 Court directed the parties to meet and confer with the goal of reducing the total length
14 of the video excerpts to no more than one minute, and the Court directed the
15 Government to consider whether still images from those videos would suffice in
16 presenting its case. (*Id.* at 8-9.)

17 In this manner, the Court GRANTS IN PART the Government’s Motion *in*
18 *Limine* to Admit Child Pornography Images and Videos. (Doc. 18.)

19 **II. DEFENDANT’S MOTION TO SUPPRESS EVIDENCE**

20 The defense moves to suppress Defendant’s videotaped statements made to an
21 investigator during the execution of a search warrant at Defendant’s residence.
22 (Doc. 26.) The Government filed an Opposition brief (Doc. 35), Defendant filed a
23 Reply brief (Doc. 49), and the Court held a suppression hearing. The parties filed
24 post-hearing briefs. (Docs. 69 & 76.)

25 During the early-morning execution of a search warrant at his residence on
26 February 5, 2015, Defendant was interviewed regarding his possession of child
27 pornography by Huntington Beach Police Department Detective David Syvock, but he
28 was not given *Miranda* warnings. *See Miranda v. Arizona*, 384 U.S. 436, 444 (1966).

1 As a result, Defendant contends that he was subjected to a custodial interrogation
2 without *Miranda* warnings, and that his statements must therefore be suppressed. The
3 Government maintains that the interview of Defendant was not custodial.

4 **A. Factual Findings and Credibility Determinations**

5 In ruling on a Motion to Suppress, the district court must resolve factual
6 disputes and must state its findings. Fed. R. Crim. P. 12(d) (“When factual issues are
7 involved in deciding a motion, the court must state its essential findings on the
8 record.”). In doing so, the district court may make credibility determinations. *See,*
9 *e.g., United States v. Arreguin*, 735 F.3d 1168, 1174 (9th Cir. 2013); *United States v.*
10 *Labrada-Bustamante*, 428 F.3d 1252, 1259 (9th Cir. 2005).

11 In the subsections that follow, the Court discusses its factual findings and sets
12 forth citations to the record that support those findings. The Court pauses here to
13 discuss witness credibility. For instance, the Court credits the testimony of Defendant
14 that he was told by two officers that he could not leave his residence while the search
15 warrant was being executed. Although Detective Syvock and Agent Speakman
16 testified that they did not inform Defendant that he could not leave, approximately
17 twelve other officers who did not testify at the hearing were at Defendant’s residence,
18 and any one of them could have told Defendant he was not free to leave.

19 On a number of points, the Court discredits the testimony of Detective Syvock.
20 The Court does so in light of inconsistencies between Detective Syvock’s account of
21 the events that occurred during the execution of the search warrant at Defendant’s
22 residence and other evidence, including videotaped evidence and the testimony of
23 other law enforcement officers. First, as discussed above in connection with
24 Defendant’s testimony, the Court discredits Detective Syvock’s statement in his
25 Declaration that Hartman was not “in any way restrained from leaving.” (Syvock
26 Decl. ¶ 12.)⁵ Moreover, despite Detective Syvock’s testimony to the contrary, the

27
28 ⁵ The Syvock Declaration is attached as an Exhibit to the Government’s Opposition brief. (Doc. 35-1.)

1 Court credits Defendant's testimony that Detective Syvock placed his hands behind
2 his back and held them there. (*Compare* 10/28/15 Tr. at 160 ("I did not put his hands
3 behind his back.") *with id.* at 238 (Hartman's testimony to the contrary).)⁶ The Court
4 credits Defendant's testimony because it is corroborated by the testimony of his
5 neighbor, a disinterested third-party witness. (*See* 10/27/15 Vol. II at 21-22 & 25
6 (neighbor's testimony that Defendant was handcuffed or had his hands held behind his
7 back).)⁷ The Court also discredits Detective Syvock's testimony as to whether
8 Defendant was physically restrained because Detective Syvock was unquestionably
9 incorrect about another issue related to the amount of control he exerted over
10 Defendant during his interrogation. Specifically, Detective Syvock's Declaration
11 differed from the irrefutable videotaped evidence on a central issue: whether
12 Detective Syvock was visibly armed with a handgun when he interrogated Hartman.
13 (*Compare* Syvock Decl. ¶ 14 (stating that Syvock concealed his gun during his
14 interrogation of Defendant) *with* Motion Ex. C (still images from video of
15 interrogation with both officers carrying unconcealed handguns on waist) *and*
16 10/28/15 Tr. at 138-39 (testimony regarding the inconsistency).)

17 An additional inconsistency is found between Detective Syvock's testimony
18 and that of Defendant, disinterested third-party witnesses, and two other law
19 enforcement officers, all of whom testified that Defendant was not wearing a shirt
20 when he was ordered out of his residence upon the officers' initial entry. (*Compare*
21 Syvock Decl. ¶ 7 (Defendant was outside "wearing shorts and a t-shirt") *with* 10/28/15
22 Tr. at 233 (Hartman testified he was wearing "boxer briefs") *and* 10/27/15 Tr. Vol. II
23 at 95-96 (neighbor testimony that Defendant wore only his boxers and no shirt) *and*
24 10/27/15 Tr. Vol. II at 106 (second neighbor's testimony that Defendant wore no
25 shirt) *and* 10/28/15 Tr. at 122 (Officer Bard's testimony that Defendant wore "shorts

26
27 ⁶ The October 28, 2015 Transcript is attached as an Exhibit to the Defendant's Post-Hearing brief in
support of the Motion to Suppress. (Doc. 76-2.)

28 ⁷ The October 27, 2015 Vol. II Transcript is attached as an Exhibit to the Defendant's Post-Hearing
brief in support of the Motion to Suppress. (Doc. 76-1.)

1 or boxers, or pajama[] bottoms” without a shirt) *and* 10/28/15 Tr. at (Agent
2 Speakman’s testimony that Defendant wore “boxer shorts . . . or shorts and . . . no
3 shirt.”)

4 Whether Defendant was told by an officer he couldn’t leave, whether he was
5 restrained physically by the interrogating officer at any point, and whether the
6 interrogating officer was wearing an unconcealed handgun during the interrogation are
7 all crucial facts in the Court’s determination of whether Defendant’s statements
8 should be suppressed. Detective Syvock’s testimony on these points is unreliable.
9 The last point, whether Defendant was wearing a shirt or not, is less crucial, but it is
10 still relevant, and the fact that Detective Syvock’s Declaration is inconsistent with
11 testimony of five other witnesses, including two law enforcement officers, tends to
12 underscore the unreliability of his testimony on the more important points.

13 With those initial observations regarding credibility, the Court considers
14 whether Defendant’s statements should be suppressed.

15 **B. *Miranda* Standard of Admissibility**

16 The Government may not offer as evidence those statements that are obtained
17 as a result of a custodial interrogation of the accused unless the Government can show
18 that the accused was advised of his right to remain silent, that anything he says can be
19 used against him in a court of law, that he has the right to counsel, and that if he
20 cannot afford counsel one will be appointed for him prior to questioning. *Miranda*,
21 384 U.S. at 478-79.

22 Where a suspect is not formally in police custody, a court may determine that
23 he is nevertheless “in custody” for purposes of *Miranda* where the suspect is
24 “deprived of his freedom of action in any significant way.” *Id.* at 444. In doing so, the
25 Court asks whether, in the totality of the circumstances, a reasonable person would
26 “have felt he or she was not at liberty to terminate the interrogation and leave.”
27 *Thompson v. Keohane*, 516 U.S. 99, 112 (1995).

28 The Ninth Circuit has recognized that unique “analytical challenges” are

1 presented where, as here, the interrogation at issue is conducted in the suspect's
2 residence. *United States v. Craighead*, 539 F.3d 1073, 1082-89 (9th Cir. 2008) (“[A]
3 reasonable person interrogated inside his own home may have a different
4 understanding of whether he is truly free ‘to terminate the interrogation’ if his home is
5 crawling with law enforcement agents conducting a warrant-approved search.”). In
6 considering the issue, the court in *Craighead* identified a non-exhaustive list of factors
7 courts should consider in determining whether an at-home interrogation of an accused
8 is custodial in nature. 539 F.3d at 1084. Those factors are:

9 (1) the number of law enforcement personnel and whether
10 they were armed; (2) whether the suspect was at any point
11 restrained, either by physical force or by threats; (3) whether
12 the suspect was isolated from others; and (4) whether the
13 suspect was informed that he was free to leave or terminate
14 the interview

15 *Id.* at 1084. Also relevant is “the context in which any . . . statements were made.” *Id.*
16 The Court considers these factors.

17 **C. Application of *Craighead* Factors**

18 First, the Court considers the number of law enforcement personnel and
19 whether they were armed. In *Craighead*, the court noted that the presence of a large
20 number of officers that filled the home would contribute to a finding that an
21 interrogation was custodial in nature. *Id.* Moreover, a large number of officers
22 contribute to a suspect's reasonable belief that he would be stopped if he attempted to
23 leave. *Id.* at 1084-85. Additionally, the presence of unholstered weapons may signify
24 threat of police force, and the presence of more than one law enforcement agency may
25 obscure the chain of authority such that a suspect may reasonably believe that officers
26 of one agency have no authority to speak for officers of another agency. *Id.* at 1085.

27 Here, a total of fourteen officers were assigned to execute the search warrant at
28 Defendant's residence. (10/28/15 Tr. at 136 & 153.) An entry team of eight law

1 enforcement officers entered the small apartment where Defendant lived with his
2 mother. (10/28/15 Tr. at 194; Gomez Decl. ¶ 2 (estimating the square footage of the
3 apartment at 612 square feet).) Detective Syvock testified that the apartment was so
4 small that it was unlikely that all fourteen officers would have fit in the apartment at
5 the same time. (10/28/15 Tr. at 136-37.) The number of officers involved in executing
6 the search warrant at Defendant's residence has the tendency to create the type of
7 police-dominated environment that creates a reasonable belief that one is not free to
8 leave. Indeed, Defendant testified that two officers indicated to him that he was, in
9 fact, not free to leave at all. (Hartman Decl. ¶¶ 5-6; 10/28/15 Tr. at 204-05.)⁸

10 In addition to the number of officers, this factor considers whether the officers
11 were armed. Here, the officers who entered Defendant's residence were heavily
12 armed, and Defendant was repeatedly interrogated by two officers who were visibly
13 armed with handguns. Agent Speakman was the first to enter, and he pointed a
14 military-style rifle at Defendant's chest. (Hartman Decl. ¶¶ 2-3; Speakman Decl. ¶ 8.)⁹
15 Agent Speakman testified that that the rifle was chosen for its accuracy and its ability
16 to intimidate occupants encountered when executing a search warrant. (10/28/15 Tr. at
17 188-89 (agreeing with statement that this rifle is intended to make occupants "stop in
18 their tracks").) Moreover, even after the residence was secured by a protective sweep,
19 the officers who interrogated Defendant remained visibly armed. (*See* Mot. Ex. C.) It
20 is clear that the presence of armed officers could have reasonably contributed to a
21 belief by Defendant that he was not free to leave.

22 Finally, here, as in *Craighead*, it was unclear who was in charge of the
23 execution of the search warrant. Specifically, as in *Craighead*, the fourteen officers
24 were from three separate law enforcement agencies involved in executing the search
25 warrant: the Huntington Beach Police Department, the Orange County Sheriff's
26 Department, and the United States Department of Homeland Security. (10/28/15 Tr. at
27

28 ⁸ The Hartman Declaration is attached as an Exhibit to the Motion to Suppress. (Doc. 26-1.)

⁹ The Speakman Declaration is attached as an Exhibit to the Government's Opposition. (Doc. 35-2.)

1 151.) Moreover, even Detective Syvock, who was in charge of the investigation, had
2 difficulty identifying who was in charge of operations during the execution of the
3 search warrant. (10/28/15 Tr. at 154-57.) Defendant testified he did not know who was
4 in charge at the scene, either. (10/28/15 Tr. at 207 (“No one informed me of who was
5 in charge”))

6 In sum, as to the first factor, it is clear that there were many law enforcement
7 officers in the very small space of Defendant’s residence. They entered the residence
8 led by a law enforcement officer armed with an assault rifle, and Defendant’s
9 interrogators remained armed. There was no clear discernible chain of command or
10 any identifiable officer in charge of the search warrant execution. Accordingly, this
11 first factor weighs heavily in favor of a finding of custodial interrogation.

12 Second, the Court considers whether the suspect was restrained at any time,
13 whether through physical force through the use of threats. *Craighead*, 539 F.3d at
14 1085. This includes consideration of the ability of the suspect to move around the
15 residence freely, without police escort or monitoring. *Id.* In considering this factor, it
16 is irrelevant if the measures taken by law enforcement officers are necessary
17 precautions to safely execute the search warrant. *Id.* at 1086.

18 Here, Defendant was confronted by armed police officers entering his
19 residence. (10/28/15 Tr. at 212-13.) A military rifle was pointed directly at him.
20 (10/28/15 Tr. at 188-89.) Defendant was ordered at gunpoint to put his hands up, and
21 then after he complied, he was ordered to put his hands up higher. (10/28/15 Tr. at
22 214-15.) He was escorted out of his residence, dressed only in his underwear, where
23 he remained for approximately 10 to 15 minutes. (Hartman Decl. ¶ 3; 10/28/15 Tr. at
24 233.) He was ordered not to leave when he approached the stairs. (Hartman Decl. ¶ 5;
25 10/28/15 Tr. at 204-05.) He was again ordered not to leave during a break between
26 Detective Syvock’s interrogation sessions. (Hartman Decl. ¶ 6; 10/28/15 Tr. at 204-
27 05.) He was told before the first break between interrogation sessions that he would
28 not be permitted to move around the apartment during a break in the interrogation.

1 (Gov't Opp'n Ex. A (videotaped interview at time stamp 7:43 a.m.)) Thus, it is clear
2 that Defendant was initially restrained by the threat of the use of deadly force, that his
3 movement within his residence was highly restricted, and that he was prohibited from
4 leaving the residence. Accordingly, the second factor also weighs heavily in favor of a
5 finding of custodial interrogation.

6 Third, the Court must consider the "crucial factor" of whether the suspect was
7 isolated from others. *Craighead*, 539 F.3d at 1086-87. This factor is especially
8 important because police domination of a suspect's will is less likely to occur when
9 the suspect is in the company of individuals such as family, friends, or colleagues who
10 might give moral support to the suspect or actively discourage the suspect from
11 making inculpatory statements. *Id.* at 1087. Indeed, the Ninth Circuit has suggested
12 that affirmative actions by officers to isolate the suspect from friends and family in his
13 own home may be sufficient to find that an interrogation is custodial in nature. *Id.*
14 ("The FBI may exclude whomever it chooses from an interrogation; *Miranda* requires
15 that if the FBI isolates the suspect, and the suspect does not reasonably believe he is
16 free to leave, warnings must be given.")

17 Here, Defendant was isolated from his mother, and there is no suggestion in the
18 record that Defendant was at any time given the option of having his mother present
19 during his interrogation. (Hartman Decl. ¶ 6; *cf.* 10/28/15 Tr. at 209 (Defendant
20 testified he did not ask for his mother to be present because "[he] didn't know that
21 [he] could ask that").) Detective Syvock testified that he interrogated Defendant in his
22 mother's bedroom, with the door closed, in order to protect Defendant's privacy.
23 (10/28/15 Tr. at 171; *but cf.* Syvock Decl. ¶ 9 (mother's bedroom used because this
24 was the only room not yet being searched by officers).) While Detective Syvock may
25 have indeed been motivated by the desire to protect the privacy of the accused,
26 Detective Syvock's subjective intent is not relevant to the Court's inquiry as to this
27 factor. What is relevant to the Court's inquiry is whether Defendant was in fact
28 isolated before he was interrogated. On this point, there is no dispute.

1 Defendant's isolation contributes greatly to a reasonable belief that he was not
2 free to leave or refuse to answer Detective Syvock's questions. Unlike the
3 circumstances in *Craighead*, no officer was physically blocking the door that led out
4 of the bedroom where Defendant was interrogated; however, Defendant understood
5 that just beyond the closed door, there awaited armed law enforcement officers who
6 had twice denied his attempts to leave his residence. Detective Syvock himself set up
7 the room to interrogate Defendant in isolation. Whether he intended to protect
8 Defendant's privacy or had some other subjective motive, what he actually did was
9 isolate Defendant from the sole family member present at the residence and instead
10 placed Defendant in the presence of two armed police officers who interrogated him
11 without first advising him of his right to remain silent and his right to counsel.
12 Therefore, this "crucial" third *Craighead* factor likewise weighs in favor of a finding
13 that Defendant was in custody when he was interrogated.

14 Fourth, the Court considers whether the suspect was told that he was free to
15 leave and that he could end the interview. *Craighead*, 539 F.3d at 1087-88. Here, it is
16 clear that Defendant was told on more than one occasion that he was free to leave.
17 Therefore, this factor weighs in favor of finding that Defendant was not in custody
18 when he was interrogated by Detective Syvock.

19 However, the mere fact that a suspect is told that he is free to leave is not
20 dispositive. "The *Miranda* test for custody does not ask whether the suspect was told
21 that he was free to leave; the test asks whether a reasonable person [would] have felt
22 he or she was not at liberty to terminate the interrogation and leave." *Id.* at 1088
23 (internal alteration marks, quotation marks, and citation omitted). Indeed, in
24 *Craighead*, the court found that the suspect was subjected to a custodial interrogation
25 even though he was told that he was free to leave. *Id.*

26 Here, the Court makes a similar conclusion, and on similar facts. The Court's
27 reasoning applies both to the fourth *Craighead* factor and the more general *Craighead*
28 consideration of "the context in which any . . . statements were made." 539 F.3d at

1 1084. Viewed in the totality of the circumstances, although Detective Syvock
2 informed Defendant more than once that Defendant was free to leave, all other
3 circumstances clearly communicated a contrary message.

4 Specifically, in the early morning hours of February 5, 2015, fourteen armed
5 law enforcement officers descended upon Defendant's small residence to execute the
6 search warrant. Defendant's compliance with the officers' commands was demanded
7 at gunpoint. Defendant was led outside of his residence in his underwear. Defendant
8 was prevented from leaving on two separate occasions. Defendant was not given a
9 choice before he was isolated from the only family member who was present at the
10 residence. In isolation, Defendant was interrogated by two visibly armed law
11 enforcement officers. There was no ascertainable officer in charge or evident chain of
12 command at the scene; instead, three agencies reasonably appeared to share authority
13 for the police presence at Defendant's residence. Under these circumstances, a
14 reasonable person would "have felt he or she was not at liberty to terminate the
15 interrogation and leave." *Thompson*, 516 U.S. at 112.

16 **D. Ruling**

17 The first three *Craighead* factors weigh heavily in favor of a finding that
18 Defendant was subjected to custodial interrogation without being given *Miranda*
19 warnings. The fourth factor weighs against such a finding, but as the Ninth Circuit
20 found in *Craighead*, this Court finds that verbal reassurances that Defendant was free
21 to leave were ineffective in light of the circumstances. Therefore, under the totality of
22 the circumstances, the Court concludes that Defendant was subjected to a custodial
23 interrogation during the execution of the search warrant at his residence on February
24 5, 2015. It is undisputed that Defendant was not given *Miranda* warnings; therefore,
25 the Court rules that the government may not offer as evidence any statements that
26 were obtained as a result of that interrogation.

27 The Court GRANTS Defendant's Motion to Suppress as to the statements he
28 made during the interrogation by Detective Syvock during the execution of the search

1 warrant on February 5, 2015.

2 Conversely, the Court denies the Motion to Suppress to the extent it seeks
3 exclusion of evidence other than Defendant's statements. Specifically, Defendant
4 moves to suppress "statements made by witnesses who were contacted after they were
5 identified by [Defendant] during his interrogation." (Mot. at 15.) Because the
6 *Miranda* rule is a prophylactic that sweeps beyond the actual right against compelled
7 self-incrimination, the "fruit of the poisonous tree" doctrine does not apply in every
8 instance in which *Miranda* is violated. *United States v. Patane*, 542 U.S. 630, 639
9 (2004). Thus, the fruits of statements obtained in violation of *Miranda* need not be
10 suppressed unless those statements are also found to be involuntary under the Due
11 Process Clause. *See, e.g., United States v. Preston*, 751 F.3d 1008, 1016 (9th Cir.
12 2014) (en banc) (discussing voluntariness). Defendant does not argue that his
13 statements were involuntarily obtained in violation of his due process rights, and the
14 record here does not support such a finding. Therefore, the Court DENIES the Motion
15 to Suppress to the extent it seeks suppression of any evidence other than Defendant's
16 statements.

17 **III. DEFENDANT'S MOTION TO COMPEL DISCOVERY**

18 Defendant filed a Motion to Compel Discovery. (Doc. 27.) The Government
19 filed an Opposition brief (Doc. 37), and Defendant filed a Reply brief and Supplement
20 thereto (Docs. 47 & 50). The Court held a hearing, and the parties filed Post-Hearing
21 briefs. (Docs. 68-69.)

22 **A. Defendant's Request for Discovery**

23 Pursuant to *Brady v. Maryland*, 373 U.S. 83 (1963) (requiring production of
24 exculpatory evidence), *Giglio v. United States*, 405 U.S. 150 (1972) (requiring
25 production of impeachment evidence), and Federal Rule of Criminal Procedure 16,
26 Defendant seeks discovery regarding specialized software,¹⁰ including installable

27 _____
28 ¹⁰ The defense represents that prior to the filing of the Government's Opposition brief, only one type
of software, known as Peer Spectre, had been identified as being used in the investigation. (Reply at
2 & n.1.) The other software identified by the Government in the Opposition brief is known as

1 copies of the software, used by investigators to locate and download the computer
2 files that led to the two transportation of child pornography counts in the FSI.
3 Defendant seeks discovery of the software in order to effectively cross examine the
4 law enforcement officer who used the software in the investigation that led to the
5 present charges. The Government opposes Defendant's request as seeking information
6 protected by the qualified law enforcement privilege and as overly broad.

7 **B. Standard for Disclosure**

8 The Government objects to the discovery request based upon the qualified law
9 enforcement privilege. There is a qualified government privilege to protect from
10 disclosure sensitive investigative techniques where such exclusion does not unduly
11 prejudice the defense. *United States v. Van Horn*, 789 F.2d 1492, 1507 (11th Cir.
12 1986). To obtain disclosure, a defendant must show a need for the information and
13 must show more than a "mere suspicion" that the withheld information will prove
14 "relevant and helpful" to his defense or that disclosure is essential to a fair trial.
15 *United States v. Henderson*, 241 F.3d 638, 645 (9th Cir. 2001). If the defendant does
16 so, courts must balance the public's interest in protecting the flow of information with
17 the defendant's right to prepare his or her defense. *United States v. Whitney*, 633 F.2d
18 902, 911 (9th Cir.1980); *Roviaro v. United States*, 353 U.S. 53, 62 (1957) ("Whether a
19 proper balance renders nondisclosure erroneous must depend on the particular
20 circumstances of each case, taking into consideration the crime charged, the possible
21 defenses, the possible significance of the [undisclosed evidence], and other relevant
22 factors.")

23 The Court therefore considers whether Defendant has made the threshold
24 showing that the withheld information will be relevant and helpful to his defense, or
25 that disclosure is essential to a fair trial.

26 Shareaza LE. (*Id.*) The Government represents that Peer Spectre was used to identify Defendant's IP
27 address, but that Shareaza LE was used to download the files from Defendant's computer. (Opp'n at
28 1 n.1.) The defense seeks production of both Peer Spectre and Shareaza LE. For the sake of
simplicity, the Court refers collectively to both types of software as "the software."

1 **C. Relevance and Helpfulness of Discovery Request**

2 Defendant’s consistently and specifically articulated concern regarding the
3 operation of the specialized software is its ability (or lack thereof) to limit its
4 searching to those files that are designated as “publicly available” or shareable files.
5 (*See, e.g.*, Mot. at 5 (seeking discovery regarding the software to cross-examine a
6 witness who stated that the software “reads the publicly available advertisement from
7 computers that are identifying child sexual abuse images available for distribution”);
8 Reply at 5 (identifying “the issue of whether government software has the ability to
9 access files that are not in shared folders or have been deleted”); Def.’s Post-Hr’g
10 Brief at 1-2 & Ex. B (requesting a demonstration of how the software is coded to
11 navigate files on suspect’s computer to determine whether the software accesses non-
12 shared files).)

13 Here, as explained more fully below, the head of the investigation used the
14 software to identify and download the two files that form the bases of the two
15 transportation charges. Under the facts of this case, the Government’s ability to prove
16 the first element of the transportation charges, that Defendant “knowingly
17 transported” child pornography by use of his computer, is dependent upon whether the
18 downloaded files were “publicly available.” Therefore, how reliably the software
19 distinguishes between “publicly available” and non-shared files is squarely at issue.

20 In the Government’s investigation leading to the present prosecution, as set
21 forth in the Search Warrant Affidavit (“SW Affidavit”), Detective Syvock used the
22 specialized software to identify an Internet Protocol address (“IP address”),
23 76.172.3.11, that had been identified as being associated with child pornography. (SW
24 Affidavit at 12-13.)¹¹ Detective Syvock thereafter used the specialized software to
25 connect to Defendant’s computer and download videos of child pornography by use of
26 a P2P file-sharing network. (*Id.* at 13.) Two downloaded files form the factual basis

27 _____
28 ¹¹ The Search Warrant Affidavit is attached to the Government’s Supplemental Briefing Opposing
Defendant’s Motion to Compel Discovery (“Supp’l Opp’n”) as Exhibit A. (Doc. 59-1.)

1 underlying the two counts of transportation of child pornography charged in the FSI.
2 (*See id.* at 14 & 16; *cf.* FSI at 2-3.) Other downloaded files were used to support the
3 application for the search warrant. (SW Affidavit at 12-16.) Thus, there is some
4 support for the contention that Defendant maintained computers files containing child
5 pornography as “publicly available” via a P2P file-sharing network, and that six such
6 files were “publicly available” when downloaded by law enforcement officials.

7 However, the statements made in the Search Warrant Affidavit in many
8 instances lack precision, and the Government has not refuted the defense expert’s
9 analysis that suggests the files at issue here were not designated as shareable. First,
10 although Detective Syvock’s Search Warrant Affidavit states that Defendant’s
11 computer contained files with child pornography in a “shared folder,” Detective
12 Syvock does not specifically identify the file path from which the files at issue here
13 were downloaded. In other words, he does not state that he downloaded the files at
14 issue from Defendant’s “shared folder”; instead, Detective Syvock merely states that
15 he “made a direct connection to the [Defendant’s] computer . . . and download[ed] 5
16 files this computer was making available.”¹² (*Id.*) One interpretation of the phrase
17 “files this computer was making available” could be that it means that the files were
18 found in Defendant’s “shared folder,” but this is not the only possible interpretation.
19 Thus, although the “making available” phrase is not inconsistent with the files being
20 found in the “shared folder,” the phrase is unclear, and the Search Warrant Affidavit
21 does not specify the location of the downloaded files.

22 Second, the defense expert testified that the downloaded files were not found in
23 the Defendant’s “shared folder.” Specifically, Defendant’s expert, Tami L. Loehrs, a
24 computer forensics expert, performed a forensic examination of information
25 downloaded from Defendant’s computer. (Loehrs Decl. ¶ 13.)¹³ She states that four of
26 the six files downloaded from the HP Pavilion by Detective Syvock as part of the

27 ¹² The detective makes a similar statement elsewhere in the SW Affidavit. (*Id.* at 16 (referring to a
28 file that the Defendant’s “computer was making available to share”).)

¹³ The Loehrs Declaration is attached to Defendant’s Supplement to the Reply brief. (Doc. 50-1.)

1 investigation were not among the 600 files (of 4,000 total files) designated as
2 “publicly available” files. (*Id.* ¶¶ 13-14.) Although the two remaining files were
3 designated as “publicly available,” they had not been shared since May 2014, which is
4 nearly three months before the inception of Detective Syvock’s investigation. (*Id.*
5 ¶ 14.)

6 Despite ample opportunity to do so, the Government has not refuted this
7 testimony; instead, the Government’s many criticisms of Ms. Loehrs’ opinion are
8 unrelated to the issue at hand. Although the Government takes issue with Ms. Loehrs’
9 implication that the specialized software could be used to override an individual’s file-
10 sharing settings, it does not represent that such an occurrence is impossible or
11 infeasible. (*See* Gov’t Post-Hr’g brief at 9-10.) Additionally, to the extent that the
12 Government focuses on the lack of technical support for Ms. Loehrs’ contention, the
13 software simply has not been made available for testing. (*See id.*) Further, even if the
14 defense cannot point to any other case in which a court expressed the “serious
15 concerns” with the software reported by Ms. Loehrs – an argument the Government
16 made repeatedly at the hearing – what another court has held (or failed to hold) is not
17 dispositive of the issue before this Court in this case. (*See id.*) Finally, although the
18 Government criticizes Ms. Loehrs’ “lack of precision” in failing to distinguish
19 between the aMule software and the eMule software, the Government does not link
20 this failure to the soundness of Ms. Loehrs’ opinion regarding the non-shared nature
21 of the files at issue here.¹⁴ (*See id.*; *cf.* Loehrs Decl. ¶ 14.)

22 Thus, the Court concludes that Ms. Loehrs’ expert opinion makes a sufficient
23 showing regarding the relevance and helpfulness of the discovery sought by the
24 defense. The Court must therefore balance the public’s interest in protecting the flow
25 of information against the defendant’s right to prepare his or her defense. *Whitney*,
26 633 F.2d 902, 911; *Roviaro*, 353 U.S. at 62. Certainly, the public has a strong interest

27 ¹⁴ If the Government’s point is that examination of aMule folders reveal that the files were
28 downloaded from a location on Defendant’s computer containing shared files, then it should simply
have stated and supported this argument.

1 in keeping confidential any technical information that could enable those who would
2 trade in child pornography to improve their ability to evade detection and prosecution.
3 But even this strong interest must yield to the Defendant's right to require that the
4 Government prove each and every element of each charge against him.

5 Here, the present record is devoid of any indication that the specialized software
6 cannot be used to review files that are not designated as "publicly available" files
7 because such review is impossible or is technologically infeasible.¹⁵ The record is
8 likewise silent as to whether the code of the specialized software by its terms limits
9 itself to review of "publicly available" files, or that any similar self-imposed restraint
10 is otherwise hard-coded into the software. The expert declaration filed with the
11 Defendant's Supplemental Filing shows a need for the information because it goes
12 directly to the reliability of the Government's evidence as to an element of the two
13 transportation charges.

14 In sum, the Court finds that Defendant has made a showing sufficient to
15 overcome the qualified law enforcement privilege.

16 **D. Request is not Overly Broad**

17 The Government also argues that Defendant's discovery request is overly
18 broad. (Opp'n at 10.) Defendant seeks an installable copy of the software at issue, all
19 documents regarding the software, including the software's technical specifications,
20 and all documents regarding any other software used by the Government in its
21 investigation.¹⁶ (See Motion Ex. A.) This request is admittedly broad. However, in
22 the absence of any information regarding the specialized software, and in light of the
23 fact that it appears that all of the information regarding the operation of the specialized
24

25 ¹⁵ Stated otherwise, and borrowing a particularly apt phrase from the Government, the record is
26 devoid of the suggestion that it is not possible for "the law enforcement software [to override]
27 defendant's file-sharing settings." (Gov't Post-Hr'g Opp'n at 9.)

28 ¹⁶ The Court does not understand the discovery request as seeking production of the software's
source code; rather, the defense seeks an installable version of the software used by Detective
Syvock in order to subject the software to testing under controlled conditions. (10/27/15 Vol. I Tr. at
44 (defense expert testimony regarding testing).) The Court does not today order production of the
source code.

1 software is in the custody of the Government or investigatory agencies, the breadth of
2 the discovery request is understandable. Moreover, although the parties directed the
3 Government and the defense to meet and confer regarding a software demonstration
4 that addressed the Defendant's specific concern, no such demonstration occurred.
5 According to the email attached as an Exhibit to the Defendant's Post-Hearing Brief,
6 after Defendant (again) articulated his specific concern regarding the software, the
7 Government did not respond regarding whether an appropriately tailored
8 demonstration of the software could be arranged. (Def.'s Post-Hr'g Brief Ex. B.)

9 Thus, although the discovery request is broad, it is directly relevant and
10 necessary to the defense. The Court therefore finds that the request is not overly broad
11 under the circumstances. Therefore, the Court GRANTS Defendant's Motion to
12 Compel and ORDERS production of the materials described below.

13 **E. Order to Produce Software and Related Documents**

14 The Court orders the Government to produce an installable copy of both Peer
15 Spectre and Shareaza LE used by Detective Syvock during his investigation, as well
16 as an installable copy of any other software used by Detective Syvock during his
17 investigation to identify, access, or download any files belonging to Defendant or
18 associated with the two IP addresses identified by Detective Syvock as being at issue
19 in this prosecution.

20 The installable copies shall be the same versions used by Detective Syvock, and
21 shall be produced to Defendant in a manner that permits Defendant's expert to
22 conduct the testing she described at the evidentiary hearing. (10/27/15 Vol. I Tr. at
23 44.)¹⁷

24 Additionally, as to each type of software, the Government is ordered to produce
25 any of the following documents in its possession, custody, or control, (or in the
26 possession, custody, or control of the law enforcement agencies involved in the
27

28 ¹⁷ The October 27, 2015 Volume I Transcript is attached to the Government's Post-Hearing brief as an Exhibit. (Doc. 69-1.)

1 investigation of Defendant): any documents containing or referencing software
2 technical specifications, software development and updates (including updates,
3 upgrades, and bug fixes), and software use (including user manuals, documents
4 regarding hardware requirements, and documents related to troubleshooting).

5 Production shall be made pursuant to an appropriate protective order. The
6 parties are to meet and confer regarding an acceptable protective order. Within
7 **fourteen days** of the entry of this Order, the parties shall file a stipulated protective
8 order; if the parties are unable to reach a stipulation, they are directed to file a joint
9 report setting forth their respective proposals.

10 **IV. DEFENDANT’S MOTION IN LIMINE [NO. 1] TO EXCLUDE “OTHER**
11 **ACTS” EVIDENCE**

12 Defendant seeks exclusion of his journal entries regarding text messages
13 between Defendant and an individual referred to as H.S., her testimony, any
14 discussions during Defendant’s videotaped interrogation regarding H.S., and other
15 similar discussions regarding allegations of prior inappropriate contact with minors.
16 (Mot. at 3-4.) In response, the Government represents that it will not offer this
17 evidence in its case-in-chief, but may seek introduction of such evidence if Defendant
18 “opens the door.”

19 On this representation, the Court GRANTS the Motion in Limine. In the event
20 that the Government believes that Defendant opens the door to the introduction of
21 such evidence, it may raise the issue again with the Court at trial, but it must do so out
22 of the presence of the jury.

23 **V. DEFENDANT’S MOTION TO EXCLUDE EXPERT TESTIMONY**

24 Defendant moves to exclude the expert testimony of David L. McCain pursuant
25 to Federal Rule of Criminal Procedure 16(a)(1)(G),¹⁸ Federal Rules of Evidence 104,
26 702, and 703, and *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579, 589

27 _____
28 ¹⁸ Rule 16(a)(1)(G) relates to the Government’s duties regarding the disclosure of expert witnesses.
The defense purports to move pursuant to Rule 16(a)(1)(C); however, that provision is inapplicable
to the present Motion. *See* Fed. Crim. R. P. 16 advisory committee’s note to 2002 amendment.

1 (1993). Specifically, Defendant moves to exclude McCain’s testimony regarding
2 “common terms used in child pornography file titles and their meaning.” (Mot. at 1.)
3 Defendant argues that McCain is not qualified to testify regarding this issue, and that
4 the Government failed to make the required expert disclosure pursuant to Rule
5 16(a)(1)(G). (*Id.* at 2.) The Government contends that McCain is qualified, and
6 provides additional disclosures regarding McCain’s qualifications. As set forth below,
7 the Court **DENIES** Defendant’s Motion to Exclude McCain’s testimony.

8 When requested to do so by the accused, the Government is required to make
9 expert disclosures pursuant to Rule 16(a)(1)(G). More specifically:

10 At the defendant’s request, the government must give
11 to the defendant a written summary of any [expert]
12 testimony that the government intends to use . . . during its
13 case-in-chief at trial. . . . The summary provided under this
14 subparagraph must describe the witness’s opinions, the
15 bases and reasons for those opinions, and the witness’s
16 qualifications.

17 Fed. R. Crim. P. 16(a)(1)(G).

18 The admissibility of expert testimony is governed by Federal Rule of Evidence
19 702, which permits testimony from witnesses who are experts because of their
20 “knowledge, skill, experience, training, or education,” if their testimony satisfies four
21 criteria:

- 22 (a) the expert’s scientific, technical, or other specialized
23 knowledge will help the trier of fact to understand the
24 evidence or to determine a fact in issue; (b) the testimony is
25 based on sufficient facts or data; (c) the testimony is the
26 product of reliable principles and methods; and
27 (d) the expert has reliably applied the principles and
28 methods to the facts of the case.

1 Fed. R. Evid. 702 (paragraph structure altered).

2 Under Rule 702, as interpreted by *Daubert v. Merrell Dow Pharmaceuticals,*
3 *Inc.*, the Court has been assigned a gatekeeping role with respect to expert opinions,
4 and the Court must attend to its “task of ensuring that an expert’s testimony both rests
5 on a reliable foundation and is relevant to the task at hand.” *Daubert*, 509 U.S. at 597.
6 A trial court’s “gatekeeping” obligation to admit only expert testimony that is both
7 reliable and relevant is especially important “considering the aura of authority experts
8 often exude, which can lead juries to give more weight to their testimony.” *Mukhtar v.*
9 *Cal. State Univ.*, 299 F.3d 1053, 1063-64 (9th Cir. 2002). Rule 702(a) addresses an
10 expert’s qualifications and the relevance of the opinions he or she offers, and Rule
11 702(b) relates to the foundation underlying the expert opinions. Defendant challenges
12 McCain’s qualifications under Rule 702(a) and the foundation of his anticipated
13 testimony under Rule 702(b).

14 As to the Rule 702(a) issue of McCain’s qualifications, he is a former law
15 enforcement officer who has for some time worked as a computer forensics expert.
16 (*See generally* Mot., Ex. B (McCain *curriculum vitae*.) McCain’s *curriculum vitae*
17 describes over a decade of extensive experience in forensic analysis of computers for
18 law enforcement investigations. (*Id.*) However, there are only three items that suggest
19 any involvement in child pornography cases. The first two, one in 2003 and another in
20 2013, are awards from the prosecutorial agency here, the United States Attorney’s
21 Office, for his work in two child pornography cases. (*Id.* at 2-3.) The third reference
22 mentions “child exploitation” among other entries in a description of one of the many
23 types of criminal and civil cases in which McCain has been involved. (*Id.* at 3.) Thus,
24 there is little set forth in McCain’s *curriculum vitae* that suggests any specialized
25 knowledge relating to child pornography investigations generally, and nothing at all
26 regarding the more specific topic at issue here: terms commonly used in file names
27 containing images of child pornography. This suggests McCain is not qualified to
28 testify on the challenged topic.

1 From the record, it appears that the Government first provided a description of
2 McCain's qualifications on issues arising in child pornography cases when it filed its
3 Opposition to the present Motion. From this description, the Court concludes that
4 McCain is qualified to testify on the relevant issue as a result of the specialized
5 knowledge he gained through his experience in law enforcement investigations in
6 which he has examined over 1,000 devices containing child pornography and
7 additional related materials. (Opp'n at 4.)

8 Relating to the Rule 702(b) foundation issue, nothing in the Government's
9 initial disclosure, and nothing in McCain's *curriculum vitae* sets forth a description of
10 the bases and reasons for McCain's anticipated testimony. (See Mot. Exs. A-B.)
11 Indeed, a comparison of the Government's descriptions of the anticipated testimony of
12 its three experts, which is set forth in its September 24, 2015, letter to defense counsel,
13 reveals that although the bases of the opinion testimony of the first two experts are
14 disclosed, there is no similar description of the basis of McCain's testimony. (See
15 Mot. Ex. A.) However, McCain's extensive experience in forensic analyses related to
16 child pornography investigations, as described by the Government in its Opposition,
17 provides a basis for McCain's anticipated testimony.

18 The Ninth Circuit has found similar expert testimony admissible as Rule 702(a)
19 "specialized knowledge." For instance, in *United States v. Hankey*, the Ninth Circuit
20 held that the district court did not abuse its discretion in admitting expert testimony
21 regarding street gang affiliations and rules from a law enforcement officer who had
22 extensive experience working in law enforcement activities involving gang members.
23 203 F.3d 1160, 1167-69 (9th Cir. 2000). Based on this experience, the expert could
24 testify that co-defendants were members in affiliated gangs, that a gang-enforced
25 "code of silence" prohibited a gang member from testifying against a member of an
26 affiliated gang, and that a violation of that code would result in the gang member
27 being beaten up or killed. *Id.* at 1171. This testimony was made possible by the
28 expert's extensive experience in a specialized law enforcement field. This experience

1 allowed the expert to acquire the specialized knowledge that could assist the jury in
2 understanding the evidence or in determining a fact in issue.

3 In much the same way, McCain's extensive experience in conducting
4 examinations of electronic devices containing child pornography has allowed him to
5 acquire the specialized knowledge that could assist the jury in the present case. Thus,
6 the Court concludes that Rule 702 does not require exclusion of McCain's anticipated
7 testimony, that McCain is qualified to testify on the topic of common terms used in
8 child pornography file titles and their meaning, and that his anticipated testimony on
9 this issue does not lack foundation.

10 However, Rule 16(a)(1)(G) also imposes a disclosure requirement on the
11 Government, and Defendant has argued that the Government failed to provide the
12 required notice regarding the opinions it intends to elicit at trial from McCain. In
13 making its disclosure on September 24, 2015, the Government stated only that: "We
14 anticipate that Mr. McCain will testify about peer to peer networks, including
15 Gnutella, the use of eMule and eDonkey file-sharing programs as well as common
16 terms used in child pornography file titles and their meaning." (Mot. Ex. A (09/24/15
17 Letter from Gov't to defense counsel).)

18 The Government fails to address its compliance with this requirement, which
19 the Court views as a tacit admission that the Government failed to disclose in a timely
20 manner. It appears to the Court that the Government simply used the Opposition to
21 Defendant's Motion to Exclude as its opportunity to make the required disclosure.
22 Thus, the Court considers whether the Government's failure to make a more timely
23 disclosure warrants exclusion of McCain's testimony.

24 Generally, in the absence of prejudice to the defendant, the Government's
25 failure to comply with Rule 16(a)(1)(G) does not require exclusion. *See, e.g., United*
26 *States v. Mendoza-Paz*, 286 F.3d 1104, 1111-12 (9th Cir. 2002). For instance, in
27 *Mendoza-Paz*, the Ninth Circuit held that exclusion of an expert's testimony was not
28 required even though the Government failed to disclose the expert's qualifications

1 until four days before trial and to provide the basis for the expert’s testimony until the
2 first day of trial. *Id.* In the absence of identifiable prejudice to the accused, exclusion
3 was simply not required. *Id.* at 1112. In so concluding, the Ninth Circuit looked to the
4 purpose of the expert disclosure requirement, and because the accused was provided
5 “with a fair opportunity to test the merit of the expert’s testimony through focused
6 cross-examination,” Rule 16 did not require exclusion for failure to make a more
7 timely disclosure. Fed. R. Crim. P. 16 advisory committee’s note to 1993 amendment.
8 Thus, the Court considers whether Defendant will suffer prejudice as a result of the
9 Government’s failure to make its disclosure regarding McCain earlier than the date of
10 the filing of its Opposition brief.

11 When the Government filed its Opposition brief (with the required Rule
12 16(a)(1)(G) disclosure) on October 15, 2015, this case was set for trial less than two
13 weeks later, on October 27, 2015. At a status conference held the day after the filing
14 of the Opposition brief, on October 16, 2015, the Court continued the trial date to
15 December 1, 2015 because of the need to conduct an evidentiary hearing on two
16 defense motions. Because the Court continued the trial, there is no prejudice to
17 Defendant as a result in the Government’s delay in providing the Rule 16(a)(1)(G)
18 disclosure. Therefore, this delay does not require exclusion of McCain’s testimony.

19 The Motion to Exclude Expert Testimony of David L. McCain is DENIED.

20 **VI. CONCLUSION**

21 As set forth more fully herein the Court rules on the parties’ pretrial Motions as
22 follows.

23 The Court GRANTS IN PART the Government’s Motion *in Limine* to Admit
24 Child Pornography Images and Videos. (Doc. 18.)

25 The Court GRANTS IN PART Defendant’s Motion to Suppress. (Doc. 26.)

26 The Court GRANTS Defendant’s Motion to Compel Discovery. (Doc. 27.)

27 The Court GRANTS Defendant’s Motion in Limine re “Other Acts” Evidence.
28 (Doc. 28.)

1 The Court DENIES Defendant's Motion to Exclude Expert Testimony (Doc.
2 51).

3 In light of the Court's granting of the Motion to Compel Discovery, the parties
4 are directed to meet and confer regarding a stipulation to continue the trial date that
5 permits production of the materials ordered to be produced and Defendant's testing of
6 the software. The parties are ordered to file an appropriate stipulation within seven
7 days of the entry of this Order.

8 **IT IS SO ORDERED.**

9 **DATED:** November 24, 2015

10 

11
12 The Hon. Josephine L. Staton
13 United States District Judge
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 EILEEN M. DECKER
 United States Attorney
 2 DENNISE D. WILLETT
 Assistant United States Attorney
 3 Chief, Santa Ana Branch Office
 ANNE C. GANNON
 4 Assistant United States Attorney
 California State Bar No. 214198
 5 8000 United States Courthouse
 411 West Fourth Street
 6 Santa Ana, California 92701
 Telephone: (714) 338-3548
 7 Facsimile: (714) 338-3561
 Email: Anne.Gannon@usdoj.gov

8 Attorneys for Plaintiff
 9 UNITED STATES OF AMERICA

10 UNITED STATES DISTRICT COURT
 11 FOR THE CENTRAL DISTRICT OF CALIFORNIA
 12 SOUTHERN DIVISION

13 UNITED STATES OF AMERICA,
 14 Plaintiff,
 15 v.
 16 TODD CHRISTIAN HARTMAN,
 17 Defendant.

SA CR 15-063(B)-JLS

STATUS REPORT RE: EFFORTS TO
 ARRANGE TESTING OF SOFTWARE
 PURSUANT TO THE COURT'S NOVEMBER
 24, 2015 DISCOVERY ORDER AND
 DECEMBER 15, 2015 PROTECTIVE
 ORDER; EXHIBITS

19 Plaintiff, the United States of America, through its counsel of
 20 record Assistant United States Attorney Anne C. Gannon, hereby
 21 submits a status report setting forth the government's efforts to
 22 comply with the Court's November 24, 2015 order granting defendant's
 23 motion to compel discovery ("Discovery Order"; docket #87.). The
 24 Court's December 15, 2015 Protective Order detailing the protections
 25 and procedures for the disclosure of items that were the subject of
 26 the Discovery Order included a provision that the government shall
 27 notify the Court if it is not able to accommodate a request for a

1 demonstration or testing of the Protected Software by January 8,
2 2016. (docket #94, ¶ 11.) The government has made substantial
3 progress but is requesting additional time because items pivotal to
4 the requested testing are in the possession of a non-governmental
5 entity and the government must consult with this private entity that,
6 in addition to possessing the key software and data, owns the
7 intellectual property of the software system.

8 On December 18, 2015, the government was notified by the defense
9 that its expert was requesting to conduct testing on the software the
10 week of January 18, 2016. According to the request, the expert's
11 preference was to conduct the testing at a government facility in
12 Tucson, Arizona and would need two computers and full internet
13 access. In the process of making the necessary arrangements, the
14 government obtained additional information about the legal status of
15 the software at issue, specifically, the software is a suite of tools
16 known as the Child Protection System ("CPS"). CPS is the
17 intellectual property of a private, 501(c)(3) organization, Child
18 Rescue Coalition. See Exhibit A, attached hereto. In order to
19 access and use CPS, a license issued by Child Rescue Coalition is
20 required. See Exhibit B, attached hereto. This license limits who
21 may access CPS and how the software and data can be used. Id. The
22 government consulted with a Child Rescue Coalition representative and
23 discussed whether the organization would voluntarily agree to expand
24 an existing government license or create a new license to accommodate
25 a demonstration and/or testing in this case. On January 7, 2016, the
26 defense sent the government a more detailed request that set forth a

1 testing protocol much broader than what the government had previously
2 discussed with the Child Rescue Coalition representative.

3 The government in an effort to facilitate this testing and reach
4 an accommodation with Child Rescue Coalition without additional
5 litigation is making arrangements for a conference call next week
6 with defense counsel, the government, and the Child Rescue Coalition
7 representative. To date, the government has disclosed to the defense
8 a CPS manual obtained from Child Rescue Coalition and is working with
9 the Newport Beach Police Department and counsel for the Department of
10 Homeland Security - Homeland Security Investigations to disclose
11 other responsive documents in the possession of the government. The
12 government will file a status report with the Court on or before
13 January 19, 2016 if it is not able to facilitate defendant's request.
14

15
16 Dated: 1/8/16

Respectfully submitted,

EILEEN M. DECKER
United States Attorney

DENNISE D. WILLETT
Assistant United States Attorney
Chief, Santa Ana Branch Office

20
21 /s/ Anne C. Gannon
ANNE C. GANNON
Assistant United States Attorney

22
23 Attorney for Plaintiff
UNITED STATES OF AMERICA
24
25
26
27
28

1 EILEEN M. DECKER
 United States Attorney
 2 LAWRENCE S. MIDDLETON (CA Bar No. 157866)
 Assistant United States Attorney
 3 Chief, Criminal Division
 ANNE C. GANNON (CA Bar No. 214198)
 4 Assistant United States Attorney
 1300 United States Courthouse
 5 312 North Spring Street
 Los Angeles, California 90012
 6 Telephone: (213) 894-5010
 E-mail: Lawrence.Middleton@usdoj.gov
 7 Anne.Gannon@usdoj.gov

8 Attorneys for Plaintiff
 UNITED STATES OF AMERICA

9 UNITED STATES DISTRICT COURT

10 FOR THE CENTRAL DISTRICT OF CALIFORNIA

11
 12
 13 UNITED STATES OF AMERICA,
 14 Plaintiff,
 15 v.
 16 TODD CHRISTIAN HARTMAN,
 17 Defendant.

No. SA CR 15-63-JLS
GOVERNMENT'S MOTION TO DISMISS
CASE

18
 19
 20 Pursuant to Rule 48 of the Federal Rules of Criminal Procedure,
 21 and by leave of court endorsed hereon, the United States Attorney for
 22 the Central District of California hereby moves to dismiss the above-

23 \\
 24 \\
 25 \\
 26 \\
 27 \\
 28 \\
 \

1 referenced case without prejudice as to defendant Todd Christian
2 Hartman.

3 Dated: January 20, 2016

Respectfully submitted,

4 EILEEN M. DECKER
United States Attorney

5
6 /s/

7 LAWRENCE S. MIDDLETON
Assistant United States Attorney
Chief, Criminal Division

8 ANNE C. GANNON
9 Assistant United States Attorney

10 Attorneys for Plaintiff
11 UNITED STATES OF AMERICA
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28