

APPENDIX TABLE OF CONTENTS

OPINIONS AND ORDERS

Memorandum Opinion, U.S. Court of Appeals for the Ninth Circuit (February 22, 2024)	1a
Jury Verdict, U.S. District Court for the District of Montana (July 13, 2022)	7a
Memorandum Order, U.S. District Court for the District of Montana (April 22, 2022)	11a

OTHER DOCUMENT

Indictment (July 28, 2021)	36a
-------------------------------------	-----

**MEMORANDUM* OPINION, U.S. COURT OF
APPEALS FOR THE NINTH CIRCUIT
(FEBRUARY 22, 2024)**

NOT FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

TAUREAN JEROME WEBER,

Defendant-Appellant.

No. 22-30191

Appeal from the United States District Court
for the District of Montana
Dana L. Christensen, District Judge, Presiding

Argued and Submitted February 9, 2024
Portland, Oregon

Before: GOULD, BYBEE, and BRESS,
Circuit Judges.

* This disposition is not appropriate for publication and is not precedent except as provided by Ninth Circuit Rule 36-3.

Taureen Weber was convicted of eight counts of transportation, distribution, and receipt of child pornography in violation of 18 U.S.C. §§ 2252A(a)(1), 2252(a)(2), following a jury trial. Police began investigating Weber after Instagram submitted a series of CyberTips through the National Center for Missing and Exploited Children (“NCMEC”) indicating that Instagram accounts later identified as belonging to Weber contained child pornography. On appeal, Weber argues the district court erred in denying his motion to suppress evidence because a detective viewed the media attached to the CyberTips without a warrant. He also contends the district court erred in denying his motion to dismiss on speedy trial grounds and by permitting the government to ask guilt-assuming hypotheticals to certain witnesses. We have jurisdiction pursuant to 28 U.S.C. § 1291, and we affirm.

1. We affirm the district court’s denial of Weber’s motion to suppress. “In reviewing a denial of a motion to suppress, we review the district court’s factual findings for clear error and its legal conclusions *de novo*.” *United States v. Rosenow*, 50 F.4th 715, 728 (9th Cir. 2022) (citation omitted), *cert. denied*, 143 S. Ct. 786 (2023). On appeal, Weber presses only a *Jones*-style trespass theory of the Fourth Amendment and does not argue that he had a reasonable expectation of privacy in the contents of his Instagram account.

We need not decide whether the trespass theory applies to searches of electronic information, because the disclosure of Weber’s media by Instagram to the government was licensed pursuant to Instagram’s Terms of Service. *See Florida v. Jardines*, 569 U.S. 1, 7-8 (2013); *United States v. Esqueda*, 88 F.4th 818, 830 (9th Cir. 2023). Instagram’s license here was clear

that it would extend to the dissemination of certain information to law enforcement. As a condition to using Instagram, a user must agree to Instagram “shar[ing] information about misuse or harmful content with other Facebook Companies or law enforcement.” This is not a blanket Fourth Amendment waiver. Instead, when Instagram learns of “harmful” or “deceptive” behavior, it is authorized by the Terms of Service to share that information with law enforcement. Even then, the government may access only the information collected by Instagram—it may not conduct its own, free-roaming search of a user’s account. We offer no opinion on more general terms of service, nor do we consider a license’s effect under a reasonable-expectation-of-privacy theory.

Alternatively, the good-faith exception applies even if there was a search. “The good-faith exception precludes suppression of evidence seized by officers who acted ‘in objectively reasonable reliance’ on a search warrant that is later declared invalid.” *United States v. Artis*, 919 F.3d 1123, 1133 (9th Cir. 2019) (quoting *United States v. Leon*, 468 U.S. 897, 922 (1984)). We previously held that the good-faith exception did not apply where “[t]he constitutional error was made by the officer[,] . . . not by the magistrate,” *United States v. Yasey*, 834 F.2d 782, 789 (9th Cir. 1987), but “the Supreme Court’s precedent . . . has shifted somewhat since we decided *Vasey*[,]”; *see generally Herring v. United States*, 555 U.S. 135 (2009).

In *Artis*, we recognized that the good-faith exception is not “categorically inapplicable whenever a search warrant is issued on the basis of evidence illegally obtained as a result of constitutional errors by the police.” *Artis*, 919 F.3d at 1133. Rather, the proper inquiry is “whether the police misconduct that

led to discovery of the illegally obtained evidence is itself subject to the good-faith exception. If it is, suppression of the evidence seized pursuant to the warrant will not be justified.” *Id.*

In this case, Detective Hall reasonably relied on the CyberTip report that indicated Instagram had viewed the media attachments. Acting in reliance on this information, as well as training she had received on Instagram’s policies and practices, Detective Hall viewed the media believing that she was not exceeding the scope of Instagram’s search vis-à-vis the private search doctrine. Additionally, she viewed the images prior to our holding in *Wilson*, which requires the government to demonstrate that a human being viewed the attachments in the CyberTip for the private search doctrine to apply. *United States v. Wilson*, 13 F.4th 961, 971-72 (9th Cir. 2021). Thus, the good-faith exception applies.

2. Weber also challenges the district court’s denial of his motion to dismiss for a Speedy Trial Act violation. “We review the district court’s interpretation and application of the Speedy Trial Act de novo, and . . . [its] findings of fact for clear error.” *United States v. Medina*, 524 F.3d 974, 982 (9th Cir. 2008).

In general, “the Speedy Trial Act requires that a criminal trial begin within seventy days from the date on which the indictment was filed.” *United States v. Olsen*, 995 F.3d 683, as amended 21 F.4th 1036, 1040 (9th Cir. 2022) (per curiam) (citing 18 U.S.C. § 3161(c) (1)). However, “the Act includes a long and detailed list of periods of delay that are excluded in computing” those seventy days, *Zedner v. United States*, 547 U.S. 489, 497 (2006), including delays resulting from “pretrial motions, the unavailability of essential witnesses, and

delays to which the defendant agrees.” *Olsen*, 21 F.4th at 1040-41; *see* 18 U.S.C. § 3161(h).

Weber contends that the district court violated the Speedy Trial Act by setting a trial date that would have been outside of the seventy countable days had the government not filed an additional motion that “stopped the clock.” The district court acknowledged that “it inadvertently set [the trial] for a date outside of the [then-]remaining 70-day period,” but found that the timing of the government’s motion ultimately resulted in a trial date in accordance with the Act.

The text of the Speedy Trial Act does not provide a basis for a violation unless a defendant “[wa]s not brought to trial within” seventy countable days. 18 U.S.C. § 3161(a)(2). Both parties agree that Weber was brought to trial within seventy countable days, so Weber has no basis to claim a Speedy Trial Act violation. Weber’s argument that a potential violation equates to an actual violation is unpersuasive. Further, Weber did not oppose the government’s “fortuitous” motion that stopped the clock. The unopposed continuance fell squarely within the excludable category of “delays to which the defendant agrees.” *Olsen*, 21 F.4th at 1040-41. The discovery of a near-violation is not actionable under the Speedy Trial Act.

3. Lastly, Weber contends that the district court erred in allowing the government to ask guilt-assuming hypotheticals to certain witnesses. “[I]t is error for the prosecution to ask questions on cross-examination that assume the defendant’s guilt of the precise acts for which he is on trial.” *United States v. Shwayder*, 312 F.3d 1109, 1120 (9th Cir. 2002). We assume without deciding that the guilt-assuming hypotheticals were error, but we conclude that the errors were harmless.

Because guilt-assuming hypotheticals implicate due process concerns, the government bears the burden of demonstrating that any error was harmless beyond a reasonable doubt. *United States v. Evans*, 728 F.3d 953, 959 (9th Cir. 2013). Contrary to Weber's contentions that these witnesses were critical to his defense, we conclude that whatever harm these hypothetical questions might have inflicted on Weber's credibility was eclipsed by the government's overwhelming evidence of Weber's guilt. We are persuaded that the jury would have convicted Weber even in the absence of these statements given the thousands of images and videos of child pornography located in his home office, the government's evidence connecting the Instagram accounts to his email accounts, as well as the IP address information related to his electronic devices. The witnesses—who had close personal relationships with Weber—had no firsthand knowledge of the facts underlying the offense, and their testimony about Weber's good moral character was of minimal probative value. Therefore, any error was harmless.

For these reasons, we AFFIRM the judgement of the district court.

**JURY VERDICT,
U.S. DISTRICT COURT FOR THE
DISTRICT OF MONTANA
(JULY 13, 2022)**

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MONTANA
MISSOULA DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

TAUREAN JEROME WEBER,

Defendant.

CR 21-28-M-DLC

VERDICT FORM

1. We, the Jury in the above-entitled matter, unanimously find the defendant, TAUREAN JEROME WEBER:

Guilty

of transportation of child pornography, as charged in Count I of the Indictment.

2. We, the Jury in the above-entitled matter, unanimously find the defendant, TAUREAN JEROME WEBER:

Guilty

of transportation of child pornography, as charged in Count II of the Indictment.

3. We, the Jury in the above-entitled matter, unanimously find the defendant, TAUREAN JEROME WEBER:

Guilty

of transportation of child pornography, as charged in Count III of the Indictment.

4. We, the Jury in the above-entitled matter, unanimously find the defendant, TAUREAN JEROME WEBER:

Guilty

of transportation of child pornography, as charged in Count IV of the Indictment.

5. We, the Jury in the above-entitled matter, unanimously find the defendant, TAUREAN JEROME WEBER:

Guilty

of distribution of child pornography, as charged in Count VI of the Indictment.

6. We, the Jury in the above-entitled matter, unanimously find the defendant, TAUREAN JEROME WEBER:

Guilty

of distribution of child pornography, as charged in Count VII of the Indictment.

7. We, the Jury in the above-entitled matter, unanimously find the defendant, TAUREAN JEROME WEBER:

Guilty

of distribution of child pornography, as charged in Count VIII of the Indictment.

8. We, the Jury in the above-entitled matter, unanimously find the defendant, TAUREAN JEROME WEBER:

Guilty

of receipt of child pornography, as charged in Count X of the Indictment.

FORFEITURE ALLEGATION VERDICT

Having found the defendant guilty of one or more Counts in the indictment:

1. We, the Jury in the above-entitled matter find by a preponderance of the evidence that the property described as a black Cooler Master computer tower was used to facilitate the commission of the crime of Receipt of Child Pornography as charged in Count X of the Indictment:

True

2. We, the Jury in the above-entitled matter find by a preponderance of the evidence that the property described as a black Seagate desktop drive was used to facilitate the commission of the crime of Receipt of Child Pornography as charged in Count X of the Indictment:

True

3. We, the Jury in the above-entitled matter find by a preponderance of the evidence that the property described as a black Dell XPS laptop computer was used to facilitate the commission of the crime of Receipt of Child Pornography as charged in Count X of the Indictment

True

Please have the foreperson sign and date this Verdict Form and notify the bailiff you have completed your deliberation.

Signed: XXXX

Foreperson (Printed Name): XXXX

Dated: XXXXXXXX

**MEMORANDUM ORDER,
U.S. DISTRICT COURT FOR THE
DISTRICT OF MONTANA
(APRIL 22, 2022)**

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MONTANA
MISSOULA DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

TAUREAN JEROME WEBER,

Defendant.

CR 21-28-M-DLC

Before: Dana L. CHRISTENSEN,
U.S. District Judge.

Before the Court is Defendant Taurean Jerome Weber's motion to suppress and motion in limine. (Docs. 44; 46.) Mr. Weber's suppression motion argues all evidence in this case should be excluded because it is the fruit of an unconstitutional search, wherein law enforcement viewed video and image files pulled from Mr. Weber's Instagram accounts and included with several CyberTips. Mr. Weber's motion in limine seeks approval of an *Old Chief* type stipulation that the

media files at issue in this case meet the federal definition of child pornography. For the reasons stated herein, both motions will be denied.

FACTUAL BACKGROUND¹

Instagram is social media company through which users register for accounts capable of uploading, sharing, and viewing videos and images both publicly and privately. To obtain an account, one must, among other things, provide some personal information, select a username, and agree to terms of service.

It appears Mr. Weber maintained several Instagram accounts. When creating these accounts, Mr. Weber agreed to certain terms of service, which provided in relevant part that:

We also have teams and systems that work to combat abuse and violations of our Terms and policies, as well as harmful and deceptive behavior. We use all the information we have—including your information—to try to keep our platform secure. We also may share information about misuse or harmful content with other Facebook Companies or law enforcement

(Doc. 52 at 1.) These terms of service also stated that an Instagram account cannot be used for an unlawful

¹ This factual background is derived from all relevant filings and the evidence received during the suppression hearing. To the extent any “factual issues are involved in deciding” the pending motions, this background constitutes the Court’s “essential findings” of fact. *See Fed. R. Crim. P. 12(d)*.

purpose and that it has the right to remove any shared content if it violates the terms of service. (*Id.* at 3-4.)

Instagram suspected at least some of Mr. Weber's accounts housed apparent child pornography and shut those accounts down. Mr. Weber and Instagram exchanged communications regarding these accounts following their deactivation. To understand what happened next, one must understand the legal framework under which electronic service providers report suspected child pornography to the National Center for Missing and Exploited Children ("NCMEC"). Under federal law, "electronic communication service providers" need not actively search for child pornography on their platforms, but they must report it when they find it. *See* 18 U.S.C. § 2258A(f)(3). Such reports must be made to NCMEC, and, important for this case, must include the "visual depiction of apparent child pornography or other content relating to the incident such report is regarding." *Id.* § 2258A(b)(4).

Once a report is received, federal law requires NCMEC to "forward[] what is known as a CyberTip to the appropriate law enforcement agency for possible investigation." *United States v. Wilson*, 13 F.4th 961, 964 (9th Cir. 2021); *see also* 18 U.S.C. § 2258A(c). This CyberTip must include the content of the underlying report, which, as noted above, will contain the "visual depiction of apparent child pornography" forming the basis of the report. 18 U.S.C. § 2258A(b)(4), (c). The receiving law enforcement agency will then presumably launch an investigation that, at some point, will involve reviewing the media files of suspected child pornography included along with the report.

In this case, Instagram made five reports to NCMEC between late 2019 and early 2020 regarding

suspected child pornography found on the deactivated accounts created by Mr. Weber. NCMEC, in turn, sent five CyberTips to Montana law enforcement. The first CyberTip was based on information supplied to NCMEC by Instagram on October 25, 2019. (*See generally* Doc. 50-1 at 1-8.) According to the CyberTip, Instagram reported that an account with the username “lordgonnor” and email address lordgonnor@gmail.com contained suspected child pornography. (*Id.* at 3.) The account’s IP address was associated with geolocation data in the Missoula, Montana area. (*Id.* at 5.) This report and corresponding CyberTip contained one video file and one image file, both of which Instagram indicated it had viewed. (*Id.* at 3-4.) NCMEC also indicated one of its staff members had viewed the files. (*Id.* at 7.) CyberTip 1 was sent to Gary Seder, then-commander of Montana’s Internet Crimes Against Children task force on December 6, 2019. (*Id.* at 6.)

The second CyberTip was based on information supplied to NCMEC by Instagram on November 29, 2019. (*See generally id.* at 9-15.) According to the CyberTip, Instagram reported that an account with the username “ggshoutouts2020” and email address lordgonnor+insta@gmail.com contained suspected child pornography. (*Id.* at 11.) The account’s IP address was associated with geolocation data in the Missoula, Montana area. (*Id.* at 13.) The report and corresponding CyberTip contained two video files and one image file, with Instagram indicating it had viewed all of these files. (*Id.* at 11-12.) NCMEC also indicated one of its staff members had viewed the files. (*Id.* at 14.) CyberTip 2 was transmitted to Gary Seder on December 6, 2019. (*Id.* at 15.)

The third CyberTip was based on information provided to NCMEC by Instagram on November 4, 2019. (*See generally id.* at 16-22.) According to the CyberTip, Instagram reported that an account with the username “_teenshoutouts2020” and email address lordgonnor+insta2@gmail.com contained suspected child pornography. (*Id.* at 18.) The account’s IP address was associated with geolocation data in the Missoula, Montana area. (*Id.* at 20.) The report and corresponding CyberTip contained one video file and one image file, with Instagram indicating it had viewed both of these files. (*Id.* at 18-19.) NCMEC also indicated one of its staff members had viewed the files. (*Id.* at 21.) CyberTip 3 was transmitted to Gary Seder on December 6, 2019. (*Id.* at 22.)

The fourth CyberTip was based on information provided to NCMEC by Instagram on December 9, 2019. (*See generally id.* at 23-30.) According to the CyberTip, Instagram reported that an account with the username “johnny.5.isalive” and email address lordgonnor+fxck.instagram@gmail.com contained suspected child pornography. (*Id.* at 25.) The account’s IP address was associated with geolocation data in the Missoula, Montana area. (*Id.* at 27.) The report and corresponding CyberTip contained one video file and one image file, with Instagram indicating it had viewed both of these files. (*Id.* at 25-26.) NCMEC also indicated one of its staff members had viewed the files. (*Id.* at 28.) CyberTip 4 was transmitted to Gary Seder on January 22, 2020. (*Id.* at 30.)

The fifth CyberTip was based on information provided to NCMEC by Instagram on May 23, 2020. (*See generally Doc. 50-2 at 1-11.*) According to the CyberTip, Instagram reported that an account with the username

“johnny.5.isdead” and email address lordgonnor+fanpage@gmail.com contained suspected child pornography. (*Id.* at 3.) The account’s IP address was associated with geolocation data in the Missoula, Montana area. (*Id.* at 7.) The report and corresponding CyberTip contained two image files, but, importantly, this time *Instagram did not indicate whether it had viewed these files.* (*Id.* at 4-5.) NCMEC made clear it had also not viewed the files. (*Id.* at 8-9.) CyberTip 5 was transmitted to Gary Seder on June 24, 2020. (*Id.* at 11.)

With these CyberTips in hand, law enforcement began to investigate. In this case, Gary Seder sent some of the CyberTips off for additional FBI analysis, but they all eventually made their way to Katherine Hall, a detective with the Missoula Police Department. Critically, upon receiving the CyberTips Detective Hall, without a warrant, personally viewed the media files transmitted along with them. Detective Hall did not get a warrant because not only did four of the CyberTips specifically indicate Instagram had viewed the files, but her training had taught her that Instagram, unlike some other electronic service providers, had a policy of viewing images of suspected child pornography before sending them off to NCMEC. Detective Hall’s investigation also revealed the precise residential address for the IP address associated with the reported Instagram accounts and the people that lived there. This included Mr. Weber. Detective Hall began applying for search warrants.

Between July 27, 2020 and February 17, 2021, numerous search warrants were issued and served on Mr. Weber’s house, personal effects, vehicles, electronic accounts, and electronic devices. (*See generally* Docs. 50-3; 50-4; 50-5; 50-6.) Eventually, on July 28, 2021,

Mr. Weber was indicted on five counts of transportation of child pornography, in violation of 18 U.S.C. § 2252A (a)(1) (Counts I-V) and five counts of distribution and receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2) (Counts VI-X). (Doc. 2.) On December 29, 2021, upon the United States motion, this Court dismissed Counts V and IX. (Doc. 49.) These counts related to the fifth CyberTip.

PROCEDURAL BACKGROUND

During pretrial proceedings, Mr. Weber sought information regarding how Instagram viewed the image and video files prior to transmitting them to NCMEC. To this end, the Court issued a subpoena directing Instagram to identify the employee who viewed the media files at issue or the process by which such media was viewed. (Docs. 38-1.) Instagram did not respond, and it remains unknown whether when Instagram indicated it had “viewed” the files at issue, it meant an actual human being looked at the files before they were submitted to NCMEC. Seizing on this knowledge gap, Mr. Weber seeks the suppression of every piece of evidence in this case on the basis that it is the fruit of an unconstitutional search—mainly, Detective Hall’s warrantless viewing of the image and video files included with the CyberTips.

The Court held a hearing on this motion. (Doc. 52.) During that hearing, the United States offered testimony from Detective Hall, much of which is recounted in the factual background above. Mr. Weber also filed a motion in limine. This motion requests an in limine ruling from the Court that the United States must accept his stipulation that the image and video

files at issue in this case are child pornography. For the reasons stated below, the Court denies both motions.

ANALYSIS

I. Suppression Motion

Mr. Weber's suppression motion raises several difficult questions. As an initial matter, the Court must determine whether what occurred in this case was a search, such that the Fourth Amendment's warrant requirement applies. Assuming a search did occur, the Court must then determine whether it can be saved by the private search exception as interpreted in *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021). Finally, assuming again a search did occur, and *Wilson* forecloses application of the private search exception, the Court must then determine whether the good faith exception applies. The Court will address each issue in turn.

A. Was there a search?

The Fourth Amendment forbids unreasonable searches and seizures. U.S. Const. amend. IV. "The basic purpose of this Amendment . . . is to safeguard the privacy and security of individuals against arbitrary invasions by government officials." *Carpenter v. United States*, ___ U.S. ___, ___, 138 S.Ct. 2206, 2213 (2018) (internal citations and quotation marks omitted). Over time, two doctrines have emerged regarding whether something is a "search," such that the Fourth Amendment is triggered. *United States v. Jones*, 565 U.S. 400, 404-09 (2012). Mr. Weber's motion invokes both theories in arguing that law enforcement's viewing of the

image and video files found on his Instagram accounts was a search violating the Fourth Amendment.

The first doctrine is actually the newer of the two but given its dominance over Fourth Amendment analysis in recent history, it makes sense to address it first. Under this doctrine, whether a search has occurred under the Fourth Amendment turns on the *Katz* test, which asks whether “the individual manifested a subjective expectation of privacy in the object of the challenged search, and society is willing to recognize that expectation as reasonable.” *Kyllo v. United States*, 533 U.S. 27, 32-33 (2001) (internal citations and quotation marks omitted). But, in *Jones*, the Supreme Court “changed the jurisprudential landscape by holding that this was not the exclusive rubric.” *United States v. Thomas*, 726 F.3d 1086, 1092 (9th Cir. 2013).

Instead, in *Jones* the Supreme Court breathed new life into what this Court will categorize as the second doctrine governing whether a governmental action rises to the level of a Fourth Amendment search. This doctrine is “property-based” and stems from the Fourth Amendment’s roots in “common-law trespass.” *Carpenter*, 138 S.Ct. at 2213. The focus is whether a state actor has physically intruded into private property “for the purpose of obtaining information.” *Jones*, 565 U.S. at 404-05. In other words, if “the Government obtains information by physically intruding on persons, houses, papers, or effects, a search within the original meaning of the Fourth Amendment has undoubtedly occurred.” *United States v. Thomas*, 726 F.3d 1086, 1092 (9th Cir. 2013) (internal citations and quotation marks omitted).

Mr. Weber argues that application of either of these search-tests compels the conclusion that law

enforcement's viewing of the video and image files forwarded along with the CyberTip was a search under the Fourth Amendment. (Doc. 45 at 6-10.) Specifically, Mr. Weber maintains he has both a property interest and expectation of privacy in the Instagram accounts within which the image and video files were found. At the hearing, the United States argued that the terms of service Mr. Weber agreed to when creating the Instagram accounts at issue, and Instagram deactivation of those accounts, eroded any property interest or expectation of privacy he had in their contents. The Court agrees with the United States.

The Court finds Mr. Weber's theory hits a snag almost right away. Critically, in this case law enforcement did not intrude itself into Mr. Weber's Instagram accounts at all. Instead, *Instagram* occasioned the intrusion and then turned such information over to NCMEC in fulfilment of its statutory obligations. NCMEC then did what it is legally obligated to do and transmitted that information to law enforcement. Only then did law enforcement view the image and video files at issue, and such a viewing did not occur through a direct inspection of private areas of Mr. Weber's Instagram accounts, but rather through looking at copies of image and video files included with the CyberTips.

And because nobody asserts Instagram is a state actor, Mr. Weber cannot complain that its actions violated the Fourth Amendment, because the Fourth Amendment does not apply to private conduct. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). As a general matter, when a private party transmits suspected contraband to law enforcement, they need not "avert their eyes." *Coolidge v. New Hampshire*, 403 U.S. 443, 489 (1971). But the Court finds Mr. Weber's threshold

Fourth Amendment challenge cannot be dismissed so readily, because it directly implicates the United States' attempt to avail itself of the private search exception.

Setting *Wilson*'s core holding aside, which will be discussed at length in the next section, the Court finds that it must determine whether *Instagram*'s intrusion into Mr. Weber's Instagram accounts would have constituted a search under the Fourth Amendment had it been accomplished by law enforcement. This is because the private search exception only applies when "a private party's intrusions would have constituted a search had the government conducted it and the material discovered by the private party then comes into the government's possession." *Wilson*, 13 F.4th at 967 (emphasis added). In other words, the United States does not even need the private search exception, unless it can be said that *Instagram*'s inspection of Mr. Weber's accounts constituted a search, in the constitutional sense (assuming its actions were performed by a state actor).

The Court finds that given the specific factual context of this case, *Instagram*'s intrusion into Mr. Weber's Instagram accounts would not have been a search for Fourth Amendment purposes, had it been done by law enforcement. To be sure, and as the United States recognizes, Mr. Weber enjoyed at least some privacy interest in his Instagram accounts. (Doc. 50 at 8-9.) But importantly, whether someone can assert a subjective expectation of privacy in their social media accounts depends on the privacy settings they had in place at the time the intrusion occurred. *United States v. Chavez*, 423 F. Supp. 3d 194, 201-06 (W.D. N.C. 2019) (defendant has subjective expectation of privacy in information on Facebook account he attempted "to

exclude the public” from seeing and that expectation is objectively reasonable); *but see United States v. Meregildo*, 883 F. Supp. 2d 523, 525-26 (S.D. N.Y. 2012) (no expectation of privacy in Facebook posts shared with “friends”); *United States v. Khan*, 2017 WL 2362572, *8 (N.D. Ill. 2017) (no expectation of privacy in Facebook account not invoking any privacy settings); *United States v. Westley*, 2018 WL 3448161, *5-6 (D. Conn. 2018) (same).

The problem for Mr. Weber in this case is a lack of information. Mr. Weber, not the United States, bears the burden of establishing he has a subjective expectation of privacy in the content of his Instagram accounts. *United States v. Sarkisian*, 197 F.3d 966, 986 (9th Cir. 1999). But he has not introduced any evidence regarding whether the image and video files found on his accounts by Instagram were in public or private parts of his accounts. Nor has he demonstrated whether or not they had been shared with other users, either through a direct message or posting. All of this information is critical to a *Katz* analysis in this case, and, without it, Mr. Weber cannot meet his burden of establishing he had manifested a subjective expectation of privacy in the Instagram accounts at issue. *See Westley*, 2018 WL 3448161 at *6 (holding that defendants failed to meet their burden under *Katz* when they failed to provide “affidavits or any other facts concerning the privacy settings on their Facebook accounts or any steps they took to keep their Facebook content private”). This informational gap regarding the extent to which Mr. Weber sought to make the content of his Instagram accounts private prevents the Court from concluding that a search occurred here under the *Katz* test.

Even if the Court had such evidence, the terms of service imposed by Instagram in this case likely rendered any subjective expectation of privacy objectively unreasonable. As enumerated above, the terms of service Mr. Weber agreed to when creating the Instagram accounts at issue informed him that Instagram was monitoring his content and may provide such content to law enforcement in certain situations. Given these terms of service, the Court agrees with the United States any expectation of privacy he could have had was likely rendered unreasonable given what he agreed to when creating the accounts. In sum, Mr. Weber has not met his burden in establishing that he manifested a subjective expectation of privacy in the video and image files found on his Instagram account.

Mr. Weber's property-based Fourth Amendment argument fairs no better. "The Fourth Amendment indicates with some precision the places and things encompassed by its protections: persons, houses, papers, and effects." *Florida v. Jardines*, 569 U.S. 1, 6 (2013). And in *Jones*, the Supreme Court was clear that the trespassory-focus it renewed, only extended to searches of "those items ('persons, houses, papers, and effects') that [the Fourth Amendment] enumerates." 565 U.S. at 411 n.8; *see also Patel v. City of Montclair*, 798 F.3d 895, 898 (9th Cir. 2015) (adopting this understanding of *Jones*). Put another way, authority issued after *Jones* makes clear that "*Jones* establishes a default rule that a government intrusion with respect to the enumerated items of the Fourth Amendment, regardless of a defendant's reasonable expectation of privacy, will implicate the constitutional protection against unreasonable searches and seizures" while "*Katz* broadens

the reach of the Fourth Amendment beyond the enumerated areas to those areas where the defendant manifests a reasonable expectation of privacy.” *Patel v. City of Montclair*, 798 F.3d 895, 900 (9th Cir. 2015).

Mr. Weber appears to recognize this but argues that “social media accounts” are a “modern-day [form of] property and chattel,” such that the Fourth Amendment’s property-based approach governs intrusions into them. (Doc. 45 at 9.) The Court disagrees. In the wake of *Jones*, the Supreme Court has routinely applied the *Katz* test, at the expense of the *Jones* test, to intrusions into cyberspace. *See Riley v. California*, 573 U.S. 373, 378-403 (2014) (analyzing the warrantless inspection of cell phone data in terms of *Katz* privacy expectations, not *Jones* property intrusions); *Carpenter*, 138 S.Ct. at 2211-19 (analyzing law enforcement’s obtainment of “historical cell phone records that provide a comprehensive chronicle of the user’s past movements” in terms of privacy expectations). This makes sense given *Jones* and subsequent cases focus on the government’s physical occupation of a tangible thing, such as a vehicle, car lock, or a house and its curtilage. *Jones*, 565 U.S. at 402; *Florida*, 569 U.S. at 11-12; *Dixon*, 984 F.3d at 816.

Put another way, the Court concludes that while there may of course be Fourth Amendment implications to law enforcement’s intrusion into social media accounts, such implications arise from *Katz*’s privacy expectations test as opposed to *Jones*’ focus on trespasses to tangible property. As stated above, in this case the Court cannot conclude Instagram’s inspection of the content housed within Mr. Weber’s Instagram accounts was a search under the Fourth Amendment (as far as the private search exception is concerned), because

it lacks any evidence that Mr. Weber took steps to keep the image and video files contained within those accounts free from prying eyes. For all the Court knows they may have been publicly posted on an account with a public or private setting. Either of those facts would strongly erode the expectations of privacy at play. Without such information, however, the Court cannot find that Mr. Weber has met his burden in establishing a Fourth Amendment search occurred in this case.

This really could be the end of the matter, as far as Mr. Weber's suppression motion goes. Because the Court concludes there was not a "search" of his Instagram accounts in the constitutional sense, obtainment of a warrant before law enforcement could view the image and video files derived from Instagram's inspection of the accounts was unnecessary. Nonetheless, given *Wilson*'s import to the prosecution of child pornography offenses, the Court finds it necessary to analyze how that decision applies to the facts of this case. Accordingly, in the next section the Court assumes, for the moment, that Instagram's viewing of the image and video files on his account was a search and addresses application of the private search exception under *Wilson*.

B. The Private Search Exception

As noted above, the private search exception comes into play when "a private party's intrusions would have constituted a search had the government conducted it and the material discovered by the private party then comes into the government's possession." *Wilson*, 13 F.4th at 967 (emphasis added). Under this exception, the government may warrantlessly view

materials provided to them by private parties, provided, however, that “the government search does not exceed the scope of the private one.” *Id.* at 968. Importantly, it is the United States’ burden to prove that this exception to the Fourth Amendment’s warrant requirement applies. *Id.* at 971; *see also United States v. Scott*, 705 F.3d 410, 416-17 (9th Cir. 2012). The United States has not met its burden in this case.

The parties agree that application of the private search exception in this case turns on the Ninth Circuit’s recent interpretation of the doctrine in *Wilson*. In *Wilson*, Google reported suspected child pornography to NCMEC and transmitted “four images of apparent child pornography” uploaded as email attachments to a Gmail account. *Id.* at 964. Importantly, “[n]o one at Google had opened or viewed Wilson’s email attachments,” but instead made the report based on the result of automatic processes designed to detect the transmission of child pornography. *Id.*

Under this system, Google has employees view images suspected to be child pornography and, if confirmed be such an image, assigns it a hash value and places that hash value in a “repository of hashes.” *Id.* at 964-65. If the hash value of an image uploaded to a Google account matches a hash value in the repository, a report to NCMEC is made. *Id.* at 965. A hash value match occurred with some photos uploaded to one of Wilson’s Gmail accounts and a report was made to NCMEC. *Id.* Critically, “a Google employee did not view the images” before they were submitted to NCMEC along with the report. *Id.* NCMEC did not view them either, but once they were transmitted to law enforcement in San Diego an investigator viewed the images without a warrant. *Id.*

After viewing the images without a warrant, the investigator determined they were child pornography, and, based on this, obtained a warrant for Wilson’s email accounts. *Id.* Execution of this warrant revealed child pornography and a warrant for his residence was eventually obtained, through which law enforcement found “thousands of images of child pornography.” *Id.* at 966. Wilson unsuccessfully sought suppression of the evidence procured through the search of his email accounts and residence in the district court. *Id.* Wilson appealed and the Ninth Circuit reversed.

The Ninth Circuit began by assuming, as the parties did, that the investigator’s review of Wilson’s “email attachments was a search within the meaning of the Fourth Amendment.” *Id.* at 967. Instead of addressing this antecedent question, the Ninth Circuit focused its attention on whether “the private search exception” permitted the investigator to view the images contained in the CyberTip without a warrant. *Id.* This exception “concerns circumstances in which a private party’s intrusions would have constituted a search had the government conducted it and the material discovered by the private party then comes into the government’s possession.” *Id.* The Ninth Circuit concluded it did not apply.

The crux of this holding was that “the government’s actions,” in having an investigator personally view the images provided by Google to NCMEC, “exceeded the limits of the private search exception.” *Id.* at 971. This conclusion was two-fold, including (1) that the investigator’s viewing of the images “allowed the government to learn new, critical information that it used first to obtain a warrant and then to prosecute Wilson;” and (2) “the government search . . . expanded the scope of”

Google's search because "no Google employee—or other person—had" actually viewed the images. *Id.* at 972. Based on these findings, the Ninth Circuit held that the investigator "violated Wilson's Fourth Amendment right to be free from unreasonable searches when he examined Wilson's email attachments without a warrant." *Id.* at 980.

Predictably, Mr. Weber likens his situation to that present in *Wilson* while the United States argues the case is distinguishable. The Court begins by recognizing that the charges stemming from CyberTip 5—the only CyberTip that indicates its associated attachments were not viewed by Instagram—have been dismissed upon motion of the United States. (Doc. 49.) Moreover, the United States has represented it will not rely on the evidence associated with those counts in proving the remaining counts. (Doc. 50 at 13-14.) Accordingly, and as the United States points out, Mr. Weber's suppression motion is moot to the extent it challenges law enforcement's viewing of the media files associated with that CyberTip. *United States v. Arias-Villanueva*, 998 F.2d 1491, 1502 (9th Cir. 1993), overruled on other grounds by *United States v. Gaudin*, 515 U.S. 506 (1995). But this does not resolve the question of how *Wilson* applies to Detective Hall's review of the remaining CyberTips.

Mr. Weber contends that because the United States cannot demonstrate whether an Instagram employee actually viewed the media files in question, and what the precise scope of that viewing was, it cannot avail itself to the private search exception in this case. (Doc. 45 at 11-12.) The United States responds that it "does not matter how the provider viewed the files—it only matters the detective was informed that the provider

did view the entire content of the video files.” (Doc. 50 at 19 (emphasis original).) The Court finds that at least as far as application of the private search exception is concerned, it is constitutionally significant that the nature of Instagram’s “viewing” of the media files attached to the CyberTips is unknown.

Although Mr. Weber obtained and served a subpoena from this Court directing Instagram to identify the employee who viewed the media files at issue or the process by which such media was viewed (Doc. 38), this information remains unknown. And such information is critical to determining whether the “viewing” that occurred in this case by Instagram was sufficiently akin to the personal viewing Detective Hall subsequently accomplished. The reality is an indication on a CyberTip that an electronic service provider viewed the media files included along with that tip is insufficient to ensure *Wilson*’s mandate has been complied with. This is illustrated by pointing out what the Court still does not know at this point.

First, the Court is unaware whether an actual human being, as opposed to an automatic process, “viewed” the media files at issue. Second, the Court has no knowledge of the precise scope of the viewing that did occur. Without either of these facts, the Court cannot conclude that the United States has met its burden in finding that the private search exception applies in this case. As such, assuming that Instagram’s inspection of Mr. Weber’s accounts did amount to a Fourth Amendment search (which, for the reasons stated above, it does not), *Wilson* would likely foreclose application of the private search exception in this case. The Court finds the good faith exception is similarly inapplicable.

C. The Good Faith Exception

The United States argues that Detective Hall's warrantless viewing of the image and video files forwarded along with the CyberTips can be justified by the good faith exception. (Doc. 50 at 20-23.) Specifically, the United States contends that Detective Hall relied in good faith on Instagram's representation in CyberTips 1-4 that it had viewed the images before sending them along to NCMEC. (*Id.*) Mr. Weber argues that good faith exception only applies to errors made by magistrates, not investigating officers. (Doc. 45 at 13-14.) The Court tends to agree with Mr. Weber.

The good faith exception was created by the Supreme Court in *United States v. Leon*, 468 U.S. 897 (1984). In *Leon*, the Supreme Court held that the exclusionary rule should not require suppression of evidence obtained by officer's acting in good faith reliance on a warrant issued by neutral and detached magistrate, even if that warrant is ultimately found to be invalid. 468 U.S. at 926. The Ninth Circuit has concluded that the good faith exception derived from *Leon* is inapplicable when the ultimately invalid warrant was issued based on tainted evidence. *United States v. Vasey*, 834 F.2d 782, 789 (9th Cir. 1987). Under *Vasey*, when the constitutional error is made by the "officer" as opposed to the "magistrate," *Leon* is inapplicable. *Id.*

For purposes of its good-faith analysis, the Court presumes, as it did in the context of the private search exception discussed above, that Detective Hall's viewing of the image and video files constituted a search requiring a warrant under the Fourth Amendment, even though, for the reasons discussed above, the Court finds that not to be the case. As *Vasey* and other cases

make clear, application of the good faith exception through *Leon* extends to situations in which law enforcement permissibly relies on judicially issued warrants, not other forms of information. *Id.*; *see also Arizona v. Evans*, 514 U.S. 1, 15 (1995) (extending *Leon* to officer's reliance on warrant entry in computer database); *United States v. Barnes*, 895 F.3d 1194, 1203-04 (9th Cir. 2018) (good faith exception applies situations where officers rely on infirm warrants).

Here, the United States entire argument for application of the good faith exception stems from Detective Hall's reliance on Instagram's representation that it had viewed the image and video files submitted along with the CyberTips. But *Vasey* teaches that, in the Ninth Circuit, the good faith exception extends only to those situations in which law enforcement relies on a judicially issued warrant. 834 F.2d at 789. Because the constitutional error that happened in this case, if any, occurred when Detective Hall warrantlessly viewed the media files included with the CyberTips, the Court finds the good faith exception inapplicable.

D. Summary of Suppression Analysis

In sum, the Court finds it must deny Mr. Weber's suppression motion because he has not demonstrated a subjective expectation of privacy in the Instagram accounts on which the media files at issue were found. Mr. Weber has not established that the files were contained in private areas of the account or that he had invoked any privacy settings to keep such files hidden. Even if he had, the Court finds that Instagram's terms of service in this case likely rendered any expectation of privacy objectively unreasonable. Because of this, the Court concludes that Instagram's inspection of

his Instagram accounts was not a search for Fourth Amendment purposes.

Based on this conclusion, the United States need not rely on the private search or good faith exceptions to the warrant requirement. And this is fortunate for the United States because the Court concludes neither exception applies in this case. As to the private search exception, the Court finds the United States has failed to meet its burden in establishing that Detective Hall's viewing of the media files included with the CyberTips did not exceed the scope of Instagram's viewing of those files. Indeed, we do not know how Instagram viewed them, whether through the eyes of a human employee or through an automatic process. Without this information, the Court cannot ensure compliance with *Wilson*. As a final matter, the Court concludes the good faith exception does not apply because Detective Hall did not rely on any information contained within a judicially issued warrant. Having addressed the arguments raised by Mr. Weber's suppression motion, the Court turns its attention to his motion in limine.

II. The Motion in Limine

“A motion in limine is a procedural mechanism to limit in advance testimony or evidence in a particular area.” *United States v. Heller*, 551 F.3d 1108, 1111 (9th Cir. 2009). Such motions do not “resolve factual disputes or weigh evidence” but rather focus on whether the evidence at issue is “inadmissible on all potential grounds.” *United States v. Meech*, 2020 WL 5517029, *4 (D. Mont. 2020) (CR 20-13-BU-DLC). In adjudicating motions in limine, this Court is afforded broad discretion. *Id.* “However, in limine rulings are

not binding” and this Court “may always change [its] mind during the course of a trial.” *Ohler v. United States*, 529 U.S. 753, 758 n.3 (2000).

Mr. Weber seeks an in limine ruling from this Court compelling the United States to accept his *Old Chief*-type stipulation that the media files at issue in this case meet the federal definition of child pornography. (Doc. 47 at 2-4.) Alternatively, Mr. Weber argues this Court should limit the number of media files the United States may show to the jury under Rule 403. (*Id.* at 5-6.) The United States resists Mr. Weber’s proffered stipulation and contends a limiting order is unnecessary in this case because the United States already intends to limit the number of media files it shows to the jury. (*Id.* at 5-17.) The Court will deny the motion.

Old Chief can be read for the narrow proposition that, given the “peculiarities of the element of felony-convict status and of admissions and the like when used to” obtain a conviction under 18 U.S.C. § 922(g)(1), if defendants stipulate to such status, evidence regarding the name or nature of their underlying felony conviction must be excluded under Rule 403. *Old Chief v. United States*, 519 U.S. 172, 191(1997). Because this ruling has not effectively translated itself to other cases or contexts, *see United States v. Allen*, 341 F.3d 870, 888 (9th Cir. 2003) (noting that in *Old Chief* the “Court was careful . . . to limit its holding to cases involving ‘proof of felon status’”), the Court declines Mr. Weber’s invitation to do so in his case.

In *Old Chief*, the Supreme Court was clear that the special rule it was announcing in the context of § 922(g)(1) prosecutions, ran against the longstanding principle that “the prosecution is entitled to prove its

case by evidence of its own choice, or, more exactly, that a criminal defendant may not stipulate or admit his way out of the full evidentiary force of the case as the Government chooses to present it.” *Id.* at 186-87. And although *Old Chief* is not totally inapplicable to this case, *United States v. Merino-Balderrama*, 146 F.3d 758, 762 (9th Cir. 1998) (reviewing evidentiary issue in child *Old Chief* sheds upon Rule 403), it does not require the United States to accept the sort of stipulation sought here.

Indeed, numerous Courts, including the Ninth Circuit, have rejected the interpretation of *Old Chief* Mr. Weber offers, especially, when, as is the case here, the proffered stipulation does not reach other elements such as knowledge. *See United States v. Storm*, 915 F. Supp. 2d 1196, 1201-02 (D. Or. 2012) (collecting cases). The Third Circuit has even gone so far as to note that “courts are in near-uniform agreement that the admission of child pornography images or videos is appropriate, even where the defendant has stipulated, or offered to stipulate, that those images or videos contained child pornography.” *United States v. Cunningham*, 694 F.3d 372, 391 (3rd Cir. 2012). The Court will follow these rulings and deny Mr. Weber’s motion in limine to the extent it seeks an order requiring the United States to accept his proposed stipulation.

The Court will also not prematurely limit the number of media files the United States may show to the jury at trial. Rule 403 may very well require such a limitation. But Mr. Weber offers no precise numerical value upon which he believes the prejudicial impact becomes too great. And the United States has represented it already intends to limit the images it will introduce at trial. If Mr. Weber believes the United

States is seeking to introduce too many media files at trial, he may renew his argument at that time.

Accordingly, IT IS ORDERED Mr. Weber's suppression motion (Doc. 44) and motion in limine (Doc. 46) are DENIED.

IT IS FURTHER ORDERED that trial in this matter is RESET for June 6, 2022 in Missoula, Montana. All associated deadlines are RESET as follows. The plea agreement deadline is reset for May 13, 2022. The JERS deadline and jury instructions and trial briefs deadlines are reset for May 27, 2022.

The Court's prior scheduling order (Doc. 24) remains in full force and effect in all other respects.

DATED this 22nd day of April, 2022.

/s/ Dana L. Christensen
United States District Judge

**INDICTMENT
(JULY 28, 2021)**

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MONTANA
MISSOULA DIVISION**

UNITED STATES OF AMERICA,

Plaintiff,

CR 21-28-M-DLC

vs.

INDICTMENT

TAUREAN JEROME WEBER,

Defendant.

TRANSPORTATION OF CHILD PORNOGRAPHY—
TITLE 18 U.S.C. § 2252A(A)(L)
(COUNTS 1-V)

(Penalty: Mandatory Minimum Five to 20 Years
Imprisonment, \$250,000 fine, five years to lifetime
supervised release, \$5,000 special assessment, and up
to \$35,000 special assessment)

DISTRIBUTION & RECEIPT OF CHILD
PORNOGRAPHY—TITLE 18 U.S.C. § 2252(A)(2)
(COUNTS VI-X)

(Penalty: Mandatory Minimum Five to 20 Years
Imprisonment, \$250,000 fine, five years to lifetime
supervised release, \$5,000 special assessment, and
up to \$35,000 special assessment)

FORFEITURE TITLE 18 U.S.C. § 2253(A)

INDICTMENT

THE GRAND JURY CHARGES:

COUNT I

That between on or about October 21, 2019, and April 30, 2020, at Missoula, in Missoula County, in the State and District of Montana, and elsewhere, the defendant, TAUREAN JEROME WEBER, knowingly transported any child pornography, via Dropbox, as defined in 18 U.S.C. § 2256(8)(A), using any means and facility of interstate and foreign commerce, and in and affecting interstate and foreign commerce by any means, including by computer, in violation of 18 U.S.C. §§ 2252A(a)(1) and (b).

COUNT II

That between on or about September 29, 2016, and October 23, 2019, at Missoula, in Missoula County, in the State and District of Montana, and elsewhere, the defendant, TAUREAN JEROME WEBER, knowingly transported any child pornography, as defined in 18 U.S.C. § 2256(8)(A), via Instagram using any means and facility of interstate and foreign commerce, and in and affecting interstate and foreign commerce by any means, including by computer, in violation of 18 U.S.C. §§ 2252A(a)(1) and (b).

COUNT III

That between on or about October 25, 2019, and November 3, 2019, at Missoula, in Missoula County, in the State and District of Montana, and elsewhere, the defendant, TAUREAN JEROME WEBER, knowingly transported any child pornography, as defined in

18 U.S.C. § 2256(8)(A), via Instagram using any means and facility of interstate and foreign commerce, and in and affecting interstate and foreign commerce by any means, including by computer, in violation of 18 U.S.C. §§ 2252A(a)(1) and (b).

COUNT IV

That between on or about November 8, 2019, and December 8, 2019, at Missoula, in Missoula County, in the State and District of Montana, and elsewhere, the defendant, TAUREAN JEROME WEBER, knowingly transported any child pornography, as defined in 18 U.S.C. § 2256(8)(A), via Instagram using any means and facility of interstate and foreign commerce, and in and affecting interstate and foreign commerce by any means, including by computer, in violation of 18 U.S.C. §§ 2252A(a)(1) and (b).

COUNT V

That between on or about December 4, 2019, and May 22, 2020, at Missoula, in Missoula County, in the State and District of Montana, and elsewhere, the defendant, TAUREAN JEROME WEBER, knowingly transported any child pornography, via Instagram, as defined in 18 U.S.C. § 2256(8)(A), using any means and facility of interstate and foreign commerce, and in and affecting interstate and foreign commerce by any means, including by computer, in violation of 18 U.S.C. §§ 2252A(a)(1) and (b).

COUNT VI

That on or about October 25, 2019, at Missoula, in Missoula County, in the State and District of Montana, the defendant, TAUREAN JEROME WEBER,

knowingly distributed any visual depiction using any means and facility of interstate and foreign commerce, including by computer, and the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A), and the visual depiction is of such conduct, in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1).

COUNT VII

That on or about November 3, 2019, at Missoula, in Missoula County, in the State and District of Montana, the defendant, TAUREAN JEROME WEBER, knowingly distributed any visual depiction using any means and facility of interstate and foreign commerce, including by computer, and the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A), and the visual depiction is of such conduct, in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1).

COUNT VIII

That on or about December 7, 2019, at Missoula, in Missoula County, in the State and District of Montana, the defendant, TAUREAN JEROME WEBER, knowingly distributed any visual depiction using any means and facility of interstate and foreign commerce, including by computer, and the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A), and the visual depiction is of such conduct, in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1).

COUNT IX

That on or about May 22, 2020, at Missoula, in Missoula County, in the State and District of Montana, the defendant, TAUREAN JEROME WEBER, knowingly distributed any visual depiction using any means and facility of interstate and foreign commerce, including by computer, and the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A), and the visual depiction is of such conduct, in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1).

COUNT X

That between approximately July 2016 and July 2020, at Missoula, in Missoula County, in the State and District of Montana, the defendant, TAUREAN JEROME WEBER, knowingly received any visual depiction using any means and facility of interstate and foreign commerce, including by computer, and the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2)(A), and the visual depiction is of such conduct, in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1).

FORFEITURE ALLEGATION

As a result of the commission of any of the crimes described above, and upon his conviction, the defendant, TAUREAN JEROME WEBER, shall forfeit to the United States, all right, title and interest in the following described property seized from his residence on July 28, 2020, that represents property used to commit the offense and property that contains any

visual depiction described in § 2253(a)(l): black Cooler Master computer tower; black Seagate desktop drive; black Dell XPS laptop computer; Maxtor hard drive (internal); cell phone (xxx-xxx-6719); and two Lexar microSD USB storage devices, pursuant to 18 U.S.C. § 2253(a).

A TRUE BILL.

Foreperson signature redacted. Original document filed under seal.

/s/ Leif M. Johnson

Acting United States Attorney

/s/ Joseph E. Thaggard

Criminal Chief Assistant U.S.
Attorney

Summons: checked (IA/Arraignment - 8/23/21 @ 1:30
p.m. w. KLD)