APPENDIX

FOR PUBLICATION
UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

United States of America, *Plaintiff - Appellee*, vs. Franklin Paul Eller, Jr., *Defendant-Appellant.*	No. 20-10425 D.C. No. 3:16-cr-08207-DGC-1 OPINION

Appeal from the United States District Court
for the District of Arizona
David G. Campbell, District Judge, Presiding

Argued and Submitted November 17, 2022
Phoenix, Arizona

Filed January 25, 2023

Before: Jay S. Bybee, John B. Owens, and Daniel P. Collins, Circuit Judges.

Opinion by Judge Owens

SUMMARY*

Criminal Law

The panel affirmed Franklin Eller Jr.'s convictions for attempted coercion and enticement of a child in violation of 18 U.S.C. §§ 2422(b) and (2), in a case in which Eller, in instant messages, negotiated with adult intermediaries in the Philippines for sexually explicit images and livecam shows involving minors.

Eller argued that there was insufficient evidence to support his convictions because "there was never any question of convincing the minors to assent to participate in the sexual activity discussed." According to Eller, the messages reveal that the only issues discussed were the costs of the shows and the specific acts requested. The panel wrote that Eller's argument conflicts with the trial record, which would permit a reasonable jury to conclude that he attempted to persuade certain minors to perform his abhorrent desires, despite some apparent hesitancy on their part, and that the children's participation in the live stream was contingent on how much Eller was willing to pay. The panel noted that, more importantly, Eller's argument ignores § 2422(b)'s focus. The panel wrote that the statute applies whether the minors are real or fictional, and an attempt through an intermediary or an undercover officer still leads to criminal liability. Whether Eller's intended victims were "willing" to engage in these acts is ultimately irrelevant—the focus always remains on the defendant's subjective intent because the statute

* This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

is designed to protect children from the act of solicitation itself. The panel concluded that, with that focus, the evidence of Eller's guilt was overwhelming.

The panel addressed Eller's challenges to the search warrant and his lifetime term of supervised release in a concurrently filed disposition.

COUNSEL

Michael L. Burke (argued), Assistant Federal Public Defender; Jon M. Sands, Federal Public Defender, Federal Public Defenders Office, Phoenix. Arizona; for Defendant-Appellant.

Peter S. Kozinets (argued), Assistant United States Attorney; Krissa M. Lanham, Appellate Division Chief; Gary M. Restaino, United States Attorney; Office of the United States Attorney; Phoenix, Arizona; for Plaintiff-Appellee.

OPINION

OWENS, Circuit Judge:

Defendant-Appellant Franklin Eller, Jr. appeals from his jury convictions for, inter alia, attempted coercion and enticement of a child in violation of 18 U.S.C. §§ 2422(b) and 2. Eller argues that there was insufficient evidence to support his convictions because the government failed to show that he attempted to persuade or entice a minor to engage in sexual

activity. We have jurisdiction under 28 U.S.C. § 1291, and we affirm.[1]

I. BACKGROUND

In 2014, federal investigators discovered instant messages in which Eller negotiated with adult intermediaries in the Philippines for sexually explicit images and livecam shows involving minors. Eller was unequivocal in making these requests—he repeatedly insisted that children appear in these videos and images, and detailed the sexual acts that they should perform for money.

For example, in one instant message exchange, Eller asked, "How many girls you say you can get for [$]80[?]," to which the intermediary responded, "2 girls and me." When Eller inquired about the two girls' ages, the intermediary told him that they were 13 and 18 years old. In response, Eller asked if the intermediary could instead "get one under 18." The intermediary initially declined Eller's request until Eller again asked if one of the 13-year-old's "attractive friends [could] join instead of [the] 18 [year-old]" and that, if not, he would "go else [sic] where." The intermediary then proposed swapping the 18-year-old with an 8-year-old child, to which Eller agreed. A Western Union transaction record from the same day shows that Eller sent $90 to a person in the Philippines. The tracking number for the money

[1] We address Eller's challenges to the search warrant and his lifetime term of supervised release in a concurrently filed memorandum disposition, in which we affirm the district court's decisions.

transfer matched the one Eller sent to the intermediary in the same instant message exchange.

In this exchange and in others with three additional Philippines-based email addresses, Eller repeatedly asked questions about the participants' ages and requested children as young as 5 years old. Eller also described the sexual acts he wanted to see, including sexual activity that would cause "marks from the pain." Following these exchanges, Eller sent money to the Philippines on at least four occasions.

After law enforcement discovered dozens of such messages, Eller was arrested and charged with four counts under 18 U.S.C. §§ 2422(b) and 2.[2] In a three-day trial, the government used the explicit instant messages to argue that Eller, through the intermediaries in the Philippines, attempted to persuade minors to engage in sexual activity, in violation of § 2422(b). The jury agreed and returned guilty verdicts on all counts. Eller timely appealed.

II. DISCUSSION

A. Standard of Review

We review claims of insufficient evidence de novo. *United States v. Tuan Ngoc Luong*, 965 F.3d 973, 980 (9th Cir. 2020). When evaluating a challenge to the sufficiency of the evidence, we determine whether, "after viewing the evidence in the light most favorable

[2] A superseding indictment also charged additional child pornography counts, but Eller has not challenged the sufficiency of the evidence as to those counts.

to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *United States v. Nevils*, 598 F.3d 1158, 1163-64 (9th Cir. 2010) (en banc)(quoting *Jackson v. Virginia*, 443 U.S. 307, 319 (1979)).

B. Elements of § 2422(b)

A § 2422(b) attempt conviction requires proof of the following beyond a reasonable doubt: the defendant must have "knowingly (1) attempted to (2) persuade, induce, entice, or coerce (3) a person under 18 years of age (4) to engage in sexual activity that would constitute a criminal offense." *United States v. McCarron*, 30 F.4th 1157, 1162 (9th Cir. 2022) (citation omitted). "An attempt conviction requires evidence that the defendant intended to violate the statute and took a substantial step toward completing the violation." *Id.* (internal quotation marks and citation omitted). "To constitute a substantial step toward the commission of a crime, the defendant's conduct must (1) advance the criminal purpose charged, and (2) provide some verification of the existence of that purpose." *Id.* (citation omitted). "Moreover, a defendant's actions must cross the line between preparation and attempt by unequivocally demonstrating that the crime will take place unless interrupted by independent circumstances." *Id.* (internal quotation marks and citation omitted).

And, as we recently held consistent with every circuit to consider this issue, § 2422(b) applies to defendants who use an intermediary in their attempt to coerce minors to engage in unlawful sexual activity. See *United States v. Macapagal*, 56 F.4th 742, 744 (9th

Cir. 2022). Because "the efficacy of § 2422(b) would be eviscerated if a potential defendant could avoid prosecution by employing an adult as an intermediary," use of an intermediary is no barrier to a § 2422(b) conviction. *Id.* at 745 (citing with approval *United States v. Murrell*, 368 F.3d 1283, 1287 (11th Cir. 2004)).

C. Sufficient Evidence Supported the § 2422(b) Convictions

In light of the explicit and repeated instant messages, it is clear that the jury got this right. Eller took numerous substantial steps in his communications with and payments to the Filipino intermediaries to obtain images and videos of minors engaging in sexual activity. *See United States v. Goetzke*, 494 F.3d 1231, 1237 (9th Cir. 2007) ("[W]hen a defendant initiates conversation with a minor, describes the sexual acts that he would like to perform on the minor, and proposes a rendezvous to perform those acts, he has crossed the line toward persuading, inducing, enticing, or coercing a minor to engage in unlawful sexual activity."); *United States v. Waqar*, 997 F.3d 481, 487-88 (2d Cir. 2021) (finding sufficient evidence for a § 2422(b) conviction where the defendant offered financial incentives to an undercover agent posing as a child to have sex with him); *United States v. Berk*, 652 F.3d 132, 140 (1st Cir. 2011) (finding that the defendant took a substantial step by communicating with whom he believed was a 12-year-old girl's father about "renting her out" and "discussing . . . graphic sexual details and prices"); *United States v. Spurlock*, 495 F.3d 1011, 1014 (8th Cir. 2007) (finding sufficient evidence because the defendant described to an

undercover agent posing as the mother of two children "his desire to perform sex acts" on her children and asked her to "tell the girls about his wishes").

Despite the extensive electronic evidence, Eller contends on appeal that he is innocent of the § 2422(b) charges, as "there was never any question of convincing the minors to assent to participate in the sexual activity discussed." Instead, according to Eller, "the messages reveal that the only issues discussed were the cost of the requested shows and the specific acts requested[.]" In other words, Eller argues that he might have been guilty of shameless price haggling, but not of attempting to persuade, induce, entice, or coerce minors, as the children were prepared to engage in these acts before Eller's instant messages.

Yet Eller's argument conflicts with the trial record, which would permit a reasonable jury to conclude that he attempted to persuade certain minors to perform his abhorrent desires, despite some apparent hesitancy on their part. Eller used money as a negotiating tool to persuade the adult intermediaries and, in turn, the children to participate in the sexual acts he described. For example, Eller asked one account holder, "How many girls you say you can get for [$]80[?]" After responding to the inquiry, the account holder agreed to Eller's request to swap an 18-year-old participant with a minor only after Eller threatened to walk away from the deal if they did not comply. In another exchange, Eller asked whether, in return for $60, a second account holder and a 10-year-old child would engage in sexual acts. Indeed, Eller's haggling concerned what these children would do in exchange for money, which is the essence of

persuasion. See United States v. Nestor, 574 F.3d 159, 162 n.4 (3d Cir. 2009) (noting that a dictionary defines "persuade" as "to move by argument, entreaty, or expostulation to a belief, position, or course of action"); United States v. Hite, 769 F.3d 1154, 1161 (D.C. Cir. 2014) (noting that a dictionary defines "persuade" as "[t]o induce or win over (a person) to an act or course of action; to draw the will of (another) to something, by inclining his judgement [sic] or desire to it; to prevail upon, to urge successfully, to do something"). Eller also asked a third account holder whether they had "talked to [the] girls" about participating in a livestream show. The account holder responded that they had not yet discussed the matter with the children because Eller never agreed to a dollar amount and thus they did not "know how many cousins and nieces [would] join." In other words, the children's participation in the livestream shows was contingent on how much Eller was willing to pay.

And more importantly, Eller's argument ignores § 2422(b)'s focus. The statute applies whether the minors are real or fictional, as in the "To Catch a Predator" scenario. *See United States v. Howard*, 766 F.3d 414, 420 (5th Cir. 2014) ("Prosecutions under 18 U.S.C. § 2422(b) ordinarily are the result of sting operations" using "an undercover police officer posing as a minor (or a minor's parent)."). There need not be any minor at all—Eller's attempt to coerce a minor to engage in unlawful activity is the crime. *See, e.g.*, *United States v. Meek*, 366 F.3d 705, 717 (9th Cir. 2004) ("[A]n actual minor victim is not required for an attempt conviction under 18 U.S.C. § 2422(b)." (citation omitted)). And, as the caselaw shows, an attempt through an intermediary or an undercover

officer still leads to criminal liability. *See Macapagal*, 56 F.4th at 745. Whether Eller's intended victims were "willing" to engage in these acts is ultimately irrelevant (much like the minors' existence in the first place)—our "focus always remains on the defendant's subjective intent because the statute is designed to protect children from the act of solicitation itself."[3] *United States v. Roman*, 795 F.3d 511, 516 (6th Cir. 2015) (internal quotation marks and citation omitted). And with that focus, the evidence of Eller's guilt, which far exceeded the passages excerpted here, was overwhelming.

Accordingly, we hold that a rational jury could have found Eller guilty of attempted coercion and enticement of a minor beyond a reasonable doubt.

AFFIRMED.

---

[3] Eller's argument that the children consented prior to his messages is also unavailing because, even if the children "could theoretically assent to sexual activity as a general proposition, [which they cannot,] they could not assent to sexual activity with [Eller] until they were aware of his existence and desire or intent to have sexual contact with them." *United States v. Caudill*, 709 F.3d 444, 446 (5th Cir. 2013).

NOT FOR PUBLICATION

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

United States of America, *Plaintiff - Appellee*, vs. Franklin Paul Eller, Jr., *Defendant-Appellant.*	No. 20-10425 D.C. No. MEMORANDUM (This disposition is not appropriate for publication and is not precedent except as provided by Ninth Circuit Rule 36-3.)

Appeal from the United States District Court
for the District of Arizona
David G. Campbell, District Judge, Presiding

Argued and Submitted November 17, 2022
Phoenix, Arizona

Before: BYBEE, OWENS, and COLLINS, Circuit Judges.

Franklin Eller, Jr. appeals from his jury convictions and sentence for attempted coercion and enticement of a minor, attempted production of child pornography, and attempted receipt of child pornography. We have jurisdiction pursuant to 28

U.S.C. § 1291. As the parties are familiar with the facts, we do not recount them here. We affirm.[1]

1. Eller argues that the district court erred in denying his motion to suppress evidence obtained pursuant to an overbroad warrant. But we need not decide whether the warrant was overbroad because, under the doctrine of severance, the district court did not need to suppress any evidence presented at trial.

The doctrine of severance allows the court to "strike from a warrant those portions that are invalid and preserve those portions that satisfy the Fourth Amendment. Only those articles seized pursuant to the invalid portions need be suppressed." *United States v. Flores*, 802 F.3d 1028, 1045 (9th Cir. 2015) (quoting *United States v. Gomez-Soto*, 723 F.2d 649, 654 (9th Cir. 1984)). Severance therefore requires "identifiable portions of the warrant [to] be sufficiently specific and particular[.]" *United States v. Spilotro*, 800 F.2d 959, 967 (9th Cir. 1986).

Flores is instructive on this issue. There, the government searched the entirety of the defendant's Facebook account and seized 11,000 pages of data pursuant to a warrant seeking evidence of conspiracy and importation of a controlled substance. 802 F.3d at 1044-45. Without reaching the issue of overbreadth, we reasoned that "the two sets of Facebook messages introduced at trial were sent on the day of Flores's arrest and thus fell well-within even the narrowest of

---

[1] Eller also challenges the sufficiency of the evidence for his attempted coercion and enticement conviction under 18 U.S.C. §§ 2422(b) and 2. We affirm that conviction in a concurrently filed published opinion.

temporal limits." *Id.* at 1045-46. Because "[n]o evidence was introduced at trial that should have been suppressed," we affirmed the district court's denial of the defendant's motion to suppress under the doctrine of severance. *Id.* at 1045.

Similarly, the district court did not need to suppress any evidence introduced at Eller's trial. As Eller concedes, the search warrant affidavit supplied probable cause to justify the search of his Yahoo account from January 1 to May 11, 2012, during which he allegedly received at least three child pornography images. The affidavit also provided a factual basis to justify the search of Eller's Yahoo data after May 11, 2012: the affidavit noted that the "seller" accounts with which Eller communicated were still active, which gives rise to a reasonable probability that Eller continued to communicate with such accounts after the specific 2012 communications that Yahoo had identified.

Thus, even if the search warrant was overbroad as to Eller's pre-2012 data, we need not decide the issue because the trial exhibits in dispute are from 2013 to 2014—a period for which the warrant affidavit gave probable cause and is therefore "sufficiently specific and particular" to support severance. *Spilotro*, 800 F.2d at 967; *see also United States v. Cardwell*, 680 F.2d 75, 79 (9th Cir. 1982) ("[I]f properly relied upon to limit the scope of the warrant, [an affidavit can] provide the information needed to limit the general nature of the warrant."); *Gomez-Soto*, 723 F.2d at 653 (applying severance after finding that a portion of the warrant was sufficiently particularized because the affidavit provided probable cause justifying the seizure). Because we may affirm a denial of a motion

to suppress "on any basis supported by the record," *United States v. McClendon*, 713 F.3d 1211, 1218 (9th Cir. 2013), the district court did not err in denying Eller's motion to suppress under the doctrine of severance.[2]

2. Eller also raises two challenges to his life term of supervised release. First, he argues that the district court erred in imposing a life term of supervised release on procedural grounds by failing to adequately explain the sentence. Because Eller failed to raise this objection at the sentencing hearing, we review for plain error. *United States v. Blinkinsop*, 606 F.3d 1110, 1114 (9th Cir. 2010).

A district court commits procedural error when it fails to adequately explain the sentence selected. United *States v. Carty*, 520 F.3d 984, 993 (9th Cir. 2008) (en banc). But here, the district court adequately explained its reasoning for Eller's life term of supervised release. During the sentencing hearing, the district court justified Eller's downward variance to fifteen-years' imprisonment followed by a lifetime of supervised release by explaining the sentence acknowledged the gravity of the offense while ensuring Eller received proper mental health treatment. The district court also considered the § 3553(a) factors when explaining its sentencing decision. *See United States v. Rusnak*, 981 F.3d 697, 711 (9th Cir. 2020) (affirming the district court's decision to vary downwards for the prison sentence and impose a life term of supervised release in part

[2] Because we affirm the district court's denial of Eller's motion to suppress, we need not address the government's additional argument that the "good-faith" exception to the exclusionary rule applies.

because it had "fully considered the 18 U.S.C. § 3553(a) factors").

Although Eller "requested a specific departure" by seeking a 60-month term of supervised release, he proffered little justification for the reduced term besides his lack of criminal history. *See Carty*, 520 F.3d at 990, 992, 995 (finding that the district court was not required to provide more than a simple explanation for imposing a sentence within the Guidelines even though the defendant requested a departure based on his lack of criminal history, available alternatives, and "his sons' need for [] a role model"). Because the district court was not required to provide more in its reasoning, it did not err, let alone plainly err.

Second, Eller challenges the length of his supervised release as substantively unreasonable. We review the substantive reasonableness of conditions of supervised release for abuse of discretion. United *States v. Daniels*, 541 F.3d 915, 924 (9th Cir. 2008).

We review the substantive reasonableness of a sentencing decision under "the totality of the circumstances." *Carty*, 520 F.3d at 993. When making sentencing decisions, district courts must consider factors such as "the history and characteristics of the defendant," 18 U.S.C. § 3553(a)(1), and "the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct," *id.* § 3553(a)(6). Although this court has never recognized a presumption of reasonableness when the sentence "accords with the Commission's view of the appropriate application of § 3553(a) in the mine run of cases," we have

recognized that such a sentence is likely reasonable. *Carty*, 520 F.3d at 994 (quoting *Rita v. United States*, 551 U.S. 338, 350-51 (2007)).

Here, Eller's life term of supervised release was substantively reasonable under the totality of the circumstances. The district court properly considered the relevant factors: the nature of the offense, Eller's mental health, the need for the sentence imposed, the range of sentences available, policy considerations, and sentencing disparities between other defendants. *See* 18 U.S.C. § 3553(a). When explaining the sentence, the district court emphasized that "clearly the solution . . . is mental health treatment, . . . not years in custody."

Although the majority of other known defendants charged with the same offense do not face lifetime supervised release, this does not indicate that Eller's sentence was substantively unreasonable. The record suggests that the district court was acutely aware of the risk of sentencing disparities and identified that risk as "the most influential" factor motivating its sentencing decision. Moreover, Eller is not similarly situated to the other known defendants who did not receive a life term of supervised release. Of the additional completed federal prosecutions resulting from this investigation, nineteen out of the twenty three supervised release terms imposed were for a fixed term of years (rather than for life), and of those nineteen defendants, eighteen had pleaded guilty to all or some charges. *See United States v. Garro*, 517 F.3d 1163, 1172 (9th Cir. 2008) (finding the defendant "not similarly situated to those with whom he compared himself because they had . . . pled guilty"). The one remaining federal defendant who did not

plead guilty was sentenced to 330 years in prison, thereby rendering the length of his supervised release obsolete. And even some defendants who pleaded guilty still received lifetime supervised release. Accordingly, the district court did not abuse its discretion in imposing a life term of supervised release.

AFFIRMED.

United States of America, *Plaintiff - Appellee*, vs. Franklin Paul Eller, Jr., *Defendant-Appellant.*	No. 20-10425 D.C. Nos. 3:16-cr-08207-DGC-1 3:16-cr-08207-DGC District of Arizona, Prescott ORDER

Before: BYBEE, OWENS, and COLLINS, Circuit Judges.

The panel has voted to deny the petition for panel rehearing. Judges Owens and Collins voted to deny the petition for rehearing en banc, and Judge Bybee so recommends.

The full court has been advised of the suggestion for rehearing en banc, and no judge has requested a vote on whether to rehear the matter en banc. Fed. R. App. P. 35.

The petition for panel rehearing and the petition for rehearing en banc are therefore DENIED.

(Case: 20-10425, 04/04/2023, ID: 12688419, DktEntry: 53, Page 1 of 1)

IN THE UNITED STATES DISTRICT COURT

United States of America, v. Franklin Paul Eller, Jr.	**JUDGMENT IN A CRIMINAL CASE** (For Offenses Committed On or After November 1, 1987) No. CR-16-08207-001-PCT-DGC Maria Teresa Weidner (AFPD) Attorney for Defendant

USM # 65366-408

THERE WAS A VERDICT OF guilty on 2/13/2020 as to Counts 1-4, 9-12, and 13-16 of the Superseding Indictment.

ACCORDINGLY, THE COURT HAS ADJUDICATED THAT THE DEFENDANT IS GUILTY OF THE FOLLOWING OFFENSE(S): violating 18 U.S.C. §2422(b) and 18 U.S.C. §2, Attempted Coercion and Enticement of a Child, a Class A Felony offense, as charged in Counts 1-4 of the Superseding Indictment; 18 U.S.C. §2251(a), 18 U.S.C. §2251(e), 18 U.S.C. §2256, and 18 U.S.C. §2, Attempted Production of Child Pornography, a Class B Felony offense, as charged in Counts 9-12 of the Superseding Indictment; 18 U.S.C. §2252(a)(2), 18 U.S.C. §2252(b)(1), and 18 U.S.C. §2256, Attempted Receipt of Child Pornography, a Class C Felony

offense, as charged in Counts 13-16 of the Superseding Indictment.

IT IS THE JUDGMENT OF THIS COURT THAT the defendant is committed to the custody of the Bureau of Prisons for a term of **ONE HUNDRED EIGHTY (180) MONTHS**, which consists of **ONE HUNDRED EIGHTY (180) MONTHS** on Counts 1-4, **ONE HUNDRED EIGHTY (180) MONTHS** on Counts 9-12 and **ONE HUNDRED EIGHTY (180) MONTHS** on Counts 13-16, all such terms to run concurrently. Upon release from imprisonment, the defendant shall be placed on supervised release for a term of **LIFE**, which consists of **LIFE** on Counts 1-4 and **LIFE** on Counts 9-16, all such terms to run concurrently.

CRIMINAL MONETARY PENALTIES

The defendant shall pay to the Clerk the following total criminal monetary penalties:

SPECIAL ASSESSMENT: $1,200.00 **FINE:** WAIVED **RESTITUTION:** N/A

The Court finds the defendant does not have the ability to pay a fine and orders the fine and the assessments pursuant to 18 U.S.C. 3014(a) and 18 U.S.C. § 2559A(a)(3) waived.

The defendant shall pay a special assessment of $1,200.00 which shall be due immediately.

The defendant shall pay a total of $1,200.00 in criminal monetary penalties, due immediately. Having assessed the defendant's ability to pay,

payments of the total criminal monetary penalties are due as follows: Balance is due in equal monthly installments of $25.00 over a period of 48 months to commence 60 days after the release from imprisonment to a term of supervised release.

If incarcerated, payment of criminal monetary penalties are due during imprisonment at a rate of not less than $25 per quarter and payment shall be made through the Bureau of Prisons' Inmate Financial Responsibility Program. Criminal monetary payments shall be made to the Clerk of U.S. District Court, Attention: Finance, Suite 130, 401 West Washington Street, SPC 1, Phoenix, Arizona 85003-2118. Payments should be credited to the various monetary penalties imposed by the Court in the priority established under 18 U.S.C. § 3612(c). The total special assessment of $1,200.00 shall be paid pursuant to Title 18, United States Code, Section 3013 for Counts 1-4, 9-12, 13-16 of the Superseding Indictment.

Payments shall be applied in the following order: (1) assessment, (2) restitution principal, (3) restitution interest, (4) AVAA assessment, (5) fine principal, (6) fine interest, (7) community restitution, (8) JVTA assessment, (9) penalties, (10) costs, including cost of prosecution and court costs.

Any unpaid balance shall become a condition of supervision and shall be paid within 90 days prior to the expiration of supervision. Until all restitutions, fines, special assessments and costs are fully paid, the defendant shall immediately notify the Clerk, U.S. District Court, of any change in name and address.

The Court hereby waives the imposition of interest and penalties on any unpaid balances.

SUPERVISED RELEASE

It is ordered that while on supervised release, the defendant must comply with the mandatory and standard conditions of supervision as adopted by this court, in General Order 17-18, which incorporates the requirements of USSG §§ 5B1.3 and 5D1.2. Of particular importance, the defendant must not commit another federal, state, or local crime during the term of supervision. Within 72 hours of sentencing or release from the custody of the Bureau of Prisons the defendant must report in person to the Probation Office in the district to which the defendant is released. The defendant must comply with the following conditions:

MANDATORY CONDITIONS

1) You must not commit another federal, state or local crime.

2) You must not unlawfully possess a controlled substance. The use or possession of marijuana, even with a physician's certification, is not permitted.

3) You must refrain from any unlawful use of a controlled substance. The use or possession of marijuana, even with a physician's certification, is not permitted. Unless suspended by the Court, you must submit to one drug test within 15 days of release from imprisonment and at least two periodic drug tests thereafter, as determined by the court.

STANDARD CONDITIONS

1) You must report to the probation office in the federal judicial district where you are authorized to reside within 72 hours of sentencing or your release from imprisonment, unless the probation officer instructs you to report to a different probation office or within a different time frame.

2) After initially reporting to the probation office, you will receive instructions from the court or the probation officer about how and when you must report to the probation officer, and you must report to the probation officer as instructed.

3) You must not knowingly leave the federal judicial district where you are authorized to reside without first getting permission from the court or the probation officer.

4) You must answer truthfully the questions asked by your probation officer.

5) You must live at a place approved by the probation officer. If you plan to change where you live or anything about your living arrangements (such as the people you live with), you must notify the probation officer at least 10 days before the change. If notifying the probation officer in advance is not possible due to unanticipated circumstances, you must notify the probation officer within 72 hours of becoming aware of a change or expected change.

6) You must allow the probation officer to visit you at any time at your home or elsewhere, and you must permit the probation officer to take any items

prohibited by the conditions of your supervision that he or she observes in plain view.

7) You must work full time (at least 30 hours per week) at a lawful type of employment, unless the probation officer excuses you from doing so. If you do not have full-time employment you must try to find full-time employment, unless the probation officer excuses you from doing so. If you plan to change where you work or anything about your work (such as your position or your job responsibilities), you must notify the probation officer at least 10 days before the change. If notifying the probation officer at least 10 days in advance is not possible due to unanticipated circumstances, you must notify the probation officer within 72 hours of becoming aware of a change or expected change.

8) You must not communicate or interact with someone you know is engaged in criminal activity. If you know someone has been convicted of a felony, you must not knowingly communicate or interact with that person without first getting the permission of the probation officer.

9) If you are arrested or questioned by a law enforcement officer, you must notify the probation officer within 72 hours.

10) You must not own, possess, or have access to a firearm, ammunition, destructive device, or dangerous weapon (i.e., anything that was designed, or was modified for, the specific purpose of causing bodily injury or death to another person such as nunchakus or tasers).

11) You must not act or make any agreement with a law enforcement agency to act as a confidential human source or informant without first getting the permission of the court.

12) If the probation officer determines that you pose a risk to another person (including an organization), the probation officer may require you to notify the person about the risk and you must comply with that instruction. The probation officer may contact the person and confirm that you have notified the person about the risk.

13) You must follow the instructions of the probation officer related to the conditions of supervision.

SPECIAL CONDITIONS

The following special conditions are in addition to the conditions of supervised release or supersede any related standard condition:

1) You must participate as instructed by the probation officer in a program of substance abuse treatment (outpatient and/or inpatient) which may include testing for substance abuse. You must contribute to the cost of treatment in an amount to be determined by the probation officer.

2) You must submit your person, property, house, residence, vehicle, papers, or office to a search conducted by a probation officer. Failure to submit to a search may be grounds for revocation of release. You must warn any other occupants that the premises may be subject to searches pursuant to this condition.

3) You must participate in a mental health assessment and participate in mental health treatment as determined to be necessary by a medical or mental health professional and follow any treatment directions by the treatment provider. You must take medicine as prescribed by a medical professional providing mental health treatment, unless you object to taking the medication, in which event you must immediately notify the probation officer. You must contribute to the cost of treatment in an amount to be determined by the probation officer.

4) You must reside at and participate in a Residential Reentry Center, a residential substance abuse treatment program, a 12-step based halfway house, a sober-living environment, or any combination thereof as approved and directed by the probation officer for up to 180 days, unless discharged earlier by the probation officer. You must follow all rules and regulations. You must contribute to programming costs in an amount determined by the probation officer.

5) You must not use or possess alcohol or alcoholic beverages.

6) You must cooperate in the collection of DNA as directed by the probation officer.

7) You must attend and participate in a sex offender treatment program and sex offense specific evaluations as approved by the probation officer. You must abide by the policies and procedures of all the treatment and evaluation providers. You must contribute to the cost of such treatment and

assessment not to exceed an amount determined to be reasonable by the probation officer based on ability to pay.

8) You must attend and participate in periodic polygraph examinations as a means to determine compliance with conditions of supervision and the requirements of your therapeutic program, as directed by the probation officer. No violation proceeding will arise solely on the result of the polygraph test. A valid Fifth Amendment refusal to answer a question during a polygraph examination will not be used as a basis for a violation proceeding. You must contribute to the cost of such polygraph examination not to exceed an amount determined to be reasonable by the probation officer based on ability to pay.

9) You must reside in a residence approved, in advance, by the probation officer. Any changes in the residence must be pre-approved by the probation officer.

10) You must not knowingly possess, view, or otherwise use material depicting sexually explicit conduct involving children, as defined by 18 USC 2256(2), and material depicting "sexually explicit conduct" involving adults, defined as explicit sexually stimulating depictions of adult sexual conduct that are deemed inappropriate by your probation officer.

11) You must register as a sex offender in compliance with all federal, state, tribal or other local laws or as ordered by the Court. Failure to comply with registration laws may result in new criminal charges.

12) You must not have contact with children under the age of 18 years without prior permission of the probation officer and must immediately report to the probation officer any unauthorized contact with children. Contact includes, but is not limited to, letters, communication devices, audio or visual devices, visits, or communication through a third party.

13) You must not utilize, by any means, any social networking forums offering an interactive, user-submitted network of friends, personal profiles, blogs, chat rooms or other environment which allows for interaction with others without prior written permission from the probation officer.

14) You must not possess any device capable of capturing and/or storing an image, or video recording device without the prior written permission of the probation officer.

15) You must submit your computers (as defined in 18 U.S.C. § 1030(e)(1)) or other electronic communications or data storage devices or media, to a search. You must warn any other people who use these computers or devices capable of accessing the Internet that the devices may be subject to searches pursuant to this condition. Failure to submit to a search may be ground for revocation of release. A probation officer may conduct a search pursuant to this condition only when reasonable suspicion exists that there is a violation of a condition of supervision and that the computer or device contains evidence of this violation. You must consent to and cooperate with the seizure and removal of any hardware and/or data storage media for further analysis by law enforcement

or the probation officer with reasonable suspicion concerning a violation of a condition of supervision or unlawful conduct. Any search will be conducted at a reasonable time and in a reasonable manner.

16) You must not possess or use a computer (including internet capable devices) with access to any "on-line computer service" at any location (including place of employment) without the prior written permission of the probation officer. This includes any Internet service provider, bulletin board system, or any other public or private network or e-mail system. You must consent, at the direction of the probation officer, to having installed on your computer(s) (as defined at 18 U.S.C. § 1030(e)(1), including internet capable devices), at your own expense, any hardware or software systems to monitor your computer use.

THE DEFENDANT IS ADVISED OF HIS RIGHT TO APPEAL BY FILING A NOTICE OF APPEAL IN WRITING WITHIN 14 DAYS OF ENTRY OF JUDGMENT.

The Court may change the conditions of probation or supervised release or extend the term of supervision, if less than the authorized maximum, at any time during the period of probation or supervised release. The Court may issue a warrant and revoke the original or any subsequent sentence for a violation occurring during the period of probation or supervised release.

The Court orders commitment to the custody of the Bureau of Prisons.

The defendant is remanded to the custody of the United States Marshal.

Date of Imposition of Sentence: **Wednesday, December 16, 2020**

Dated this 17th day of December, 2020.

David G. Campbell
Senior United States District Judge

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE SEARCH OF:
CONTENT OF, AND RECORDS
RELATING TO, ELECTRONIC ACCOUNTS
NGETKO_22@YAHOO.COM *NAHOO* ID:
NGETKO _J2;SEXY _LORRAINE05@YAHOO.COM *I*
YAHOO ID: SEXY_LORRAINE05;
CUTIERHEA_l4@YAHOO.COM/YAHOO ID:
CUTIERHEA_l4;MOUNTAINMAN007@Y AHOO.COM
I YAHOO ID: MOUNTAINMAN007;
RL_ll38@YAHOO.COM/YAHOO ID: RL_ll38;
BARONWWl@Y AHOO.COM/ YAHOO ID:
BARONWWl MAINTAINED BY YAHOO! INC.
HEADQUARTERED AT 701 FIRST A VENUE,
SUNNYVALE, CA 94043

Case: 1: 14-mj-00668
Assigned To : Magistrate Judge Alan Kay
Assign. Date : 11/14/2014
Description: Search and Seizure Warrant

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

I, Caliope Bletsis, Special Agent with the Federal Bureau of Investigation, Linthicum, Maryland, Major Case Coordination Unit, being duly sworn, hereby deposes and states as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Special Agent ("SA") with the Federal Bureau of Investigation (FBI) since December 2004, and I am currently assigned to the FBI's Violent Crimes Against Children Section, Major Case Coordination Unit ("MCCU"). I am currently

investigating federal violations concerning child pornography and the sexual exploitation of children and have gained experience through training in seminars, classes, and everyday work related to these types of investigations. I have participated in the execution of numerous warrants involving the search and seizure of computers, computer equipment, software, and electronically stored information. As a federal agent, I am authorized to investigate violations of the laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

2. I make this affidavit in support of a search warrant for records relating to the email account listed in Attachment A which is maintained by Yahoo! Inc. headquartered at 701 First Avenue, Sunnyvale, California 94089. As discussed below, the e-mail account which is the subject of this search warrant was identified through information provided by Yahoo! Inc. and the National Center for Missing and Exploited Children ("NCMEC"). I have probable cause to believe that evidence of violations of 18 U.S.C. §§ 2251 (a) and (e) (production of child pornography); 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(l) (receipt and distribution of child pornography); and 18 U.S.C. §§ 2252A(a)(S)(B) and (6)(2) (possession of child pornography) is located in and within the aforementioned accounts described below. I have reason to believe that the member accounts that are the subject of the instant application will have stored information, visual depictions and communications that are relevant to this ongoing investigation, to include evidence of the identity of the person(s) maintaining the accounts listed in Attachment A.

Thus, as outlined below, and based on my training and experience, there is probable cause to believe that evidence, fruits and/or instrumentalities of the aforementioned crimes are located in this account.

3. Because the purpose of this affidavit is to set forth only the facts necessary to establish probable cause for a search warrant for this pertinent e-mail account, I have not described all the facts and circumstances of which I am aware. Facts not set forth herein are not relied upon in support of my conclusion that probable cause exists. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other agents and witnesses. Where statements of others are set forth in this affidavit, they are set forth in substance and in part.

APPLICABLE STATUTES

4. This investigation concerns alleged violations of Title 18, United States Code§§ 2251(a) and (e) (production of child pornography); 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(l) (receipt and distribution of child pornography); and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of child pornography).

a. Title 18, United States Code, Sections 225l(a) and (e) prohibits any person from employing, using, persuading, inducing, enticing, or coercing any minor to engage in, or having a minor assist any other person to engage in, or transporting any minor in or affecting interstate or foreign commerce, with the intent that such minor engage in, any sexually explicit conduct for the purpose

of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or attempting or conspiring to do so.

b. Title 18, United States Code, Sections § 2252A(a)(2)(A) and (b)(l) prohibits a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

c. Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly

accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS RELATED TO THIS SEARCH WARRANT

5. "Child Pornography," as used herein, is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

6. "Electronic Communication Service" ("ECS"), as used herein, is defined in 18 U.S.C. § 2510(15) as any service which provides to users thereof the ability to send or receive wire or electronic communications. For example, "telephone companies and electronic mail Companies" generally act as providers of electronic

communication services. *See* S. Rep. No.99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

7. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. Regardless of whether an IP address is dynamically or statically assigned, only one device can be assigned a particular IP address at any one time.

8. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

9. The term "minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

10. "Remote Computing Service" ("RCS"), as used herein, is defined in 18 U.S.C. § 2711 (2) as the provision to the public of computer storage or processing services by means of an electronic communications system.

11. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c)

masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

12. "Short Message Service" ("SMS"), as used herein, is defined as a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone.

13. The term "visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

14. The term "computer," as defined in 18 U.S.C. §1030(e)(l), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

15. The term "webcam," as used herein, refers to a front-facing video camera that attaches to a computer or that is built into a laptop or desktop screen. It is widely used for video calling as well as to continuously monitor an activity and send it to a Web server for public or private viewing. Webcams generally have a microphone built into the unit or use the computer's microphone for audio.

BACKGROUND ON THE NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN'S CYBERTIPLINE[1]

16. NCMEC is located in Alexandria, Virginia and is the leading nonprofit organization in the U.S. working with law enforcement, families, and the professionals who serve them on issues related to missing and sexually exploited children. As part of its Congressional authorization, NCMEC has created a unique public and private partnership to build a coordinated, national response to the problem of missing and sexually exploited children, establish a missing children hotline, and serve as the national clearinghouse for information related to these issues.

17. One of the services administered by NCMEC is its CyberTipline, which serves as the national clearinghouse for leads regarding sexual exploitation crimes against children. Launched in 1998, the CyberTipline is operated in partnership with the FBI, Homeland Security Investigations, the U.S. Postal Inspection Service, the U.S. Secret Service, the Military Criminal Investigative Organizations, the Internet Crimes Against Children Task Forces, the U.S. Department of Justice's Child Exploitation and Obscenity Section, as well as other state and local law enforcement agencies.

18. Reports are made by members of the general public and by U.S. Electronic Communication Service Providers ("ESPs"), which are required by U.S. federal

[1] This description is taken from NCMEC's website at http://www.missing kids.com.

law to report "apparent child pornography" to NCMEC via the CyberTipline (18 U.S.C. §2258A) if they become aware of the content on their servers. Leads are reviewed by specially-trained analysts, who examine and evaluate the reported content, add related information that may be useful to law enforcement, use publicly-available search tools to determine the geographic location of the apparent criminal act, and ultimately provide all of the gathered information to the appropriate law enforcement agency for review and possible investigation.

19. The CyberTipline receives reports, known as CyberTip reports, on the following type of criminal conduct: possession, manufacture and distribution of child pornography; online enticement of children for sexual acts; child prostitution; sex tourism involving children; child sexual molestation by a non-family member; unsolicited obscene material sent to a child; misleading domain names; and misleading words or digital images on the Internet.

20. The CyberTip reports will vary in detail depending on the nature of the report, and which entity submits it. However, the reports will include any known information (1) relating to the identity of any individual who appears to have violated federal law by committing or attempting to commit the criminal conduct described above; (2) historical information on when or how a customer or subscriber of an ECS or RCS uploaded, transmitted, or received apparent child pornography; (3) geographical information on the involved individual or website, which may include the IP Address or verified billing address or geographic identifying information, including area

code or zip code; (4) any images of apparent child pornography; and (5) the complete communication containing any image of apparent child pornography. See 18 U.S.C. § 2258A(b). Also, as will be illustrated below, CyberTip reports can be supplemented and made in connection with other CyberTip reports.

Background Regarding Computers, The Internet, and E-mail

21. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone

calls. Any reimbursement would follow these same paths.

b. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. The four functions are production, communication, distribution, and storage.

c. Child pornographers can now transfer photographs from a camera onto a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem.[2] Because

---

[2] The File Transfer Protocol (FTP) is a protocol that defines how to transfer files from one computer to another. One example, known as "anonymous FTP," allows users who do not have a login name or password to access certain files from another computer, and copy those files to their own computer.

of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images and videos at very high resolution.

e. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Google, Inc., among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child

pornography can be found on the user's computer in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

ONLINE SEXUAL EXPLOITATION OF CHILDREN VIA WEBCAM AND THE INTERNET

22. Based on my training and experience, I know one way in which individuals currently exploit children online is through the use of webcams and live streaming of the sexual abuse of children over the Internet. This is a practice that is often utilized in the Philippines another South East Asia countries. This

practice is commonly used by individuals residing outside of the Philippines who use the Internet to make contact with child sex traffickers within the Philippines. Based on my training and conversations with other agents who have experience working child exploitation investigations with ties to the Philippines, I have learned that people outside of the Philippines will use a computer, e-mail, instant messaging chat services, and a webcam to arrange for the sexual exploitation of minors in the Philippines. The requesting individual creates the opportunity by sending payment to a third party (through an international money transfer service such as Xoom, Western Union, or Pay Pal) such as a family member or a pimp in the Philippines, who can facilitate a live show via webcam in which the child disrobes and/or performs sexually explicit acts in front of a webcam in the Philippines that is broadcast live over the Internet to the individual abroad.

23. Individuals who send money to the Philippines in exchange for a sexually explicit webcam show use various means of communicating with the minor victim or a third party over the Internet - such as e-mail and Instant Messenger programs (like Yahoo mail and Yahoo! Messenger) - in order to facilitate the shows. E-mail and Instant Messenger programs are often used to groom the minor victim and/or to negotiate and plan the webcam shows.

24. I also know that the purchasing individuals often find ways to capture the sexual abuse and exploitation, either by recording the live shows onto their computers or taking still shots of the abuse, which can also be stored on the individual's computer or a electronic storage device.

TECHNICAL INFORMATION REGARDING YAHOO

Yahoo E-mail

25. In my training and experience, I have learned that Yahoo! Inc. provides a variety of on-line services, including e-mail access, to the general public. Subscribers obtain an account by registering with Yahoo! Inc. During the registration process, Yahoo! Inc. asks subscribers to provide basic personal information. Therefore, the computers of Yahoo! Inc. are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Yahoo! Inc. subscribers) and information concerning subscribers and their use of Yahoo! Inc. services, such as account access information, e-mail transaction information, and account application information.

26. In general, an e-mail that is sent to a Yahoo! Inc. subscriber is stored in the subscriber's "mail box" on Yahoo! Inc. servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Yahoo! Inc.'s servers indefinitely. The user can move and store messages in personal folders such as a "sent folder." In recent years, Yahoo and other ISPs have provided their users with larger storage capabilities associated with the user's e-mail account. Yahoo and other ISPs have allowed users to store up to one (1) terabyte of information associated with the account on ISP servers. Based on conversations with other law enforcement officers with experience in executing and reviewing search. warrants of e-mail accounts, I have learned that search warrants for e-mail accounts and

computer systems have revealed stored e-mails sent and/or received many years prior to the date of the search.

27. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Yahoo! Inc.'s servers, and then transmitted to its end destination. Yahoo! Inc. typically saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Yahoo! Inc. server, the e-mail can remain on the system indefinitely.

28. A sent or received e-mail typically includes the content of the message (including attachments), source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message may also be saved by Yahoo! Inc. but may not include all of these categories of data.

29. A Yahoo! Inc. subscriber can also store files, including e-mails, address books, contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned by Yahoo! Inc.

30. Many subscribers to Yahoo! Inc. do not store copies of the e-mails stored in their Yahoo! Inc. account on their home computers. This is particularly true because they access their Yahoo! Inc. account through the Internet, and thus it is not necessary to copy e-mails to a home computer to use the service. Moreover, an individual may not wish to maintain particular emails or files in their residence to ensure

others with access to the computer cannot access the emails.

31. In general, e-mail providers like Yahoo! Inc. ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit card or bank account number). It is important to note that e-mail providers do not validate the personal identifying information provided by subscribers.

32. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Yahoo! Inc.'s website), and other log files that reflect usage of the account. In addition, email providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

33. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical

problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

34. In my training and experience, e-mail users often use e-mail accounts for everyday transactions because it is fast, low cost, and simple to use. People use e-mail to communicate with friends and family, manage accounts, pay bills, and conduct other online business. E-mail users often keep records of these transactions in their e-mail accounts, to include personal identifying information such as name and address.

35. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to emails, including pictures and files.

Yahoo! Messenger

36. In my training and experience, I have also learned that Yahoo! Inc. provides an on-line service called Yahoo! Messenger to the general public. Yahoo! Messenger is an instant messaging client provided by Yahoo! Instant Messaging ("IM") is a form of real-time direct text-based communication between two or more people using shared clients. The text is conveyed via devices connected over a network such as the Internet. In addition to text, Yahoo's software allows users with the most current updated versions to utilize its webcam service. This option enables users from

distances all over the world to view others who have installed a webcam on their end.

37. In order to obtain a Yahoo! Messenger account, a Yahoo e-mail account is required. The Yahoo! email user must download the Yahoo! Messenger program and sign in with the same credentials used for his/her Yahoo! e-mail account. Therefore the user is issued the same Yahoo! ID for the messenger program and the email account.

38. The terms of service for a Yahoo! Messenger account states that a user's Yahoo Messenger account is tied to that same user's Yahoo Mail account. The terms of service also notify the user that Yahoo Messenger will allow the use and the people the user communicates with to save those conversations and other information into the user's affiliated Yahoo Mail account. Yahoo! Messenger also allows you to exchange computer to computer voice calls with your online friends. If you subscribe to the "Phone In" or "Phone Out" premium services, you can also use Yahoo! Messenger to make or receive calls from regular telephones.

39. You must be a registered Yahoo user in order to use Yahoo! Messenger. Yahoo! Messenger establishes a connection to the Internet when it is active -- much like a browser does -- in order for communications to be received and transmitted.

40. You may now archive Yahoo instant messages along with Yahoo Mail messages and search them together (in addition to Voice Mail, SMS, call history, and more). For users that have elected to archive their messages, Yahoo! Messenger will now archive

messages on Yahoo servers to establish and maintain this archive. Messages stored on Yahoo servers in this manner are accessible from any computer system or device able to use the latest versions of Yahoo! Messenger for computer. You can view your Yahoo! Messenger conversation history and Yahoo Mail archive (if they are tied to the same user ID) on Yahoo! Messenger through "Conversation History" in your settings. You can turn off this feature for instant messages at any time by selecting "Do not keep a record of my conversations." Even if you choose not to save your message history, users with whom you communicate may opt to use the functionality available in their version of Yahoo! Messenger to save the communications and your conversations may be saved on Yahoo servers, just like e-mail. You can delete your archived messages by selecting the message, and clicking on the "Delete" button. However, this does not delete any of your conversations saved by other users. Yahoo may analyze instant messages you elect to archive in order to provide personally relevant product features, content, and advertising, and spam and malware detection.

41. In my training and experience, evidence of the true identity of the owner of an electronic acconnt may be found in email and/or instant messages, to include personal information, pictures, and residential or work place locations and addresses.

PROBABLE CAUSE

Background

42. On or about September 17, 2014, Xoom.com, an online international money transfer service, filed a CyberTip report with NCMEC regarding Yahoo e-mail account "HANNAH_SWEETYCOLE@YAHOO.COM/ Yahoo ID: HANNAH_SWEETYCOLE." I reviewed this report, which states in part:

> Money transfer sent using our service (xoom.com) from a sender in San Francisco to a recipient in the Philippines. The recipient's Yahoo profile picture is suspicious and depicts a young girl in a lewd act. We believe the customer may have been paying for an online webcam show.

43. On or about September 30, 2014, Yahoo Electronic Crimes Investigative Team (the "ECIT") provided a supplemental report to NCMEC outlining the results of the ECIT investigation that ensued following notice of the above Cyber Tip report by Xoom.com. I reviewed this supplemental report and learned Yahoo reported the following:

> a. The user of HANNAH_SWEETYCOLE@YAHOO.COM appeared to be coordinating the sale of sexually explicit shows and/or images of herself, her children, and other children with whom she had direct contact and recruited other women around her to engage in the same activity.[3]

[3] Based on my training and experience, I know that "shows" refers to an emerging trend of sexual exploitation of children by

Additionally, the Yahoo investigation determined these women have several customers to whom they sold their "product" on multiple occasions.

b. The user of HANNAH_SWEETYCOLE@YAHOO.COM has been actively doing shows since 2010 and has recruited other women to produce shows and/or images, including the owners of email accounts "NGETKO _22@Y AHOO.COM / Yahoo ID: NGETKO J.2" and "SEXY_ LORRAINE0S@Y AHOO.COM / Yahoo ID:SEXY_LORRAINE05";

c. Yahoo believes the owners of user accounts HANNAH_SWEETYCOLE@YAHOO.COM, NGETKO_22@YAHOO.COM/Yahoo ID: NGETKO_J.2, SEXY_LORRAINE05 @YAHOO.COM/Yahoo ID: SEXY_LORRAINE05, and another e-mail account, CUTIERHEA_l4@ YAHOO.COM I Yahoo ID: CUTIERHEA 14, are connected, live in close proximity to each other in the Philippines, and may be family members;

d. On or about September 30, 2014, Yahoo generated its own CyberTip reports to NCMEC

---

individuals exploit children in foreign countries like the Philippines via web cameras such that minors remotely produce sexually explicit material via webcam for another individual and transmit these videos/images through live streaming on the Internet. Additionally, the reference to the user of HANNAH SWEETYCOLE@ YAHOO.COM as a female not been verified and confinned by investigators at this time.

> regarding user accounts NGETKO 22@Y AHOO.COM/Yahoo ID: NGETKO_22,SEXY_LORRAINE05@YAHOO. COM/Yahoo ID: SEXY_LORRAINE05, and CUTIERHEA _14@YAHOO.COM f Yahoo ID: CUTIERHEA_ 14 (the "SUBJECT SELLER ACCOUNTS"). Yahoo also provided a list of exchanges of images they observed being sent from the SUBJECT SELLER ACCOUNTS to other Yahoo user accounts. This list included the dates/times the images were sent along with the sending/receiving accounts.

44. On November 6, 2014, a member of the Yahoo ECIT advised the FBI that the sexually explicit images of children the ECIT obtained from the SUBJECT SELLER ACCOUNTS, were observed by the ECIT on September 30, 2014, as attachments to emails inside the respective SUBJECT SELLER ACCOUNT and were listed in the table of exchanges of images. Additionally, the ECIT advised that the SUBJECT SELLER ACCOUNTS and the buyers appeared to utilize Yahoo! Messenger to discuss and negotiate the sale of the sexually explicit images of children with each buyer, and then the SUBJECT SELLER ACCOUNTS used Yahoo e-mail to actually transmit the image.

45. Review of the Cyber Tip reports regarding the SUBJECT SELLER ACCOUNTS, the list of exchanged images sent from these accounts, and the above Yahoo supplemental report, revealed the following:

SEXY LORRAINE0S@YAHOO.COM

46. Yahoo submitted a Cyber Tip report for e-mail account SEXY_LORRAINE05@YAHOO.COM. In the report, Yahoo indicated that on September 30, 2014, at 11:40:00 UTC they viewed 62 image files inside user account SEXY _LORRAINE05@Y AI-JOO.COM that were sent as email attachments. Yahoo included copies of these 62 image files, which were viewed by Yahoo employees before being included in the Cyber Tip report. Approximately 47 of the 62 image files were of children engaging in sexually explicit conduct, including the following three image files that appear to depict the same minor Asian female:

a. "P3067473.JPG," which depicts an Asian female, approximately 10- to 12-years old, naked, lying on her back on a bed with her legs spread apart, such that her vagina is exposed, and she is touching her bare vagina with her hand;

b. "P3067474.JPG," which depicts an Asian female, approximately 10- to 12- years old, naked, lying on her back on a bed with her legs spread part, exposing her bare vagina; and

c. "P3067489.JPG," which depicts an Asian female, approximately 10-to 12-years old, naked, lying on her stomach on a bed, with her legs spread apart and holding her bare buttocks with her hand such that her bare vagina and anus are exposed.

47. In each of the photos, the genitals of the minor are clearly exposed, the minor is depicted in a sexualized manor, and/or the genitals are focal point of the photo.

48. On October 7, 2014, the FBI issued a letter to Yahoo! Inc. pursuant to 18 U.S.C. 2703(f) requesting

the preservation of the account SEXY _LORRAINE05@YAHOO.COM. Based on my training and experience, such account preservation ensures that information relating to the account is not lost if the user closes the account or attempts to delete the account's contents.

. . .

BARONWWl@YAHOO.COM

59. The Yahoo list of image exchanges that Yahoo observed on September 30, 2014, listed that between approximately January 1, 2012, and May 11, 2012, user account BARONWWl@YAHOO.COM was the recipient of approximately 60 of the above 72 image file e-mail attachments sent by CUTIERHEA_l4@YAHOO.COM, including the files described above (P2142856.JPG, P3093335.JPG, and P4134230.JPG).

60. On October 7, 2014, the FBI issued a letter to Yahoo pursuant to 18 U.S.C. 2703(f) requesting the preservation of the account BARONWWl@ YAHOO.COM. Based on my training and experience, such account preservation ensures that information relating to the account is not lost if the user closes the account or attempts to delete the account's contents.

61. Per the information provided by Yahoo in their supplemental report on or about September 30, 2014, the recent login activity for the SUBJECT SELLER ACCOUNTS and HANNAH_ SWEETYCOLE@ YAHOO.COM shows these users logging in from the Philippines.

62. Yahoo ECIT indicated that each user of the SUBJECT SELLER ACCOUNTS would use Yahoo Messenger to negotiate terms of sale of images and videos of minors engaging in sexually explicit conduct with the buyers. If the buyer was interested in child pornography images, the seller would then email the child pornography in1ages to the buyer. If the buyer was interested in a child pornography video, the seller would provide the video using the Yahoo! Messenger service.

63. Yahoo ECIT reported that each user of the SUBJECT SELLER ACCOUNTS, namely NGETKO 22@YAHOO.COM/Yahoo ID: NGETKO 22, SEXY_LORRAINE05@YAHOO.COM/Yahoo ID: SEXY_LORRAINE05, and CUTIERHEA_l4@YAHOO.COM/Yahoo ID: CUTIERHEA_14 each utilized their respective Yahoo! Messenger account to negotiate the terms of the sale and then either utilized their Yahoo email accounts or messenger accounts to deliver the purchased child pornography images and/or videos.

64. Because current evidence suggests that the owners of the SUBJECT SELLER ACCOUNTS reside in the Philippines, law enforcement have not been able to ascertain the true identities of the account owners nor confirmed their residences.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

65. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(l)(A) and 2703(c)(l)(A),

by using the warrant to require Yahoo, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A and Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

REQUEST TO SEAL AND ORDER
NON-DISCLOSURE

66. I request that the Court enter an Order directing Yahoo! Inc. not to notify any person, including the subscribers or customers of the accounts listed in Attachment A, of the existence of the warrant, and the fact of application for the warrant, unless and until authorized by the Court. *See* 18 U.S.C. § 2705(b) (2012). This Court has authority under 18 U.S.C. § 2705(b) to issue "an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order." *Id.* In this case, such an order would be appropriate because the requested warrant relates to an ongoing criminal investigation and I believe notification of the existence of the warrant will seriously jeopardize the ongoing investigation as such disclosure may provide an opportunity to destroy evidence, change patterns of behavior, notify confederates, or allow confederates to flee or continue flight from prosecution.

67. It is respectfully requested that this Court order that all papers submitted in support of this application, including this affidavit, the application, the warrant, and the Order itself, be sealed until further order of the Court, except that a copy of the warrant, including its attachments, shall be served upon Yahoo! Inc. As explained above, these documents discuss an ongoing criminal investigation pursuant to foreign law in The Netherlands the details of which have not been made completely public and may jeopardize the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize the foreign investigation.

CONCLUSION

68. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on computer systems owned, maintained, controlled and/or operated by Yahoo! Inc., there exists evidence of a crime, contraband, instrumentalities, and/or fruits of violations of criminal laws as specified herein. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that the e-mail accounts described in Attachment A will contain evidence of a crime, specifically but not limited to, identification of the person who manipulated the e-mails accounts described in Attachment A which I know were used to commit the aforementioned crimes. Accordingly, a search warrant is requested. Because the warrant will be served on Yahoo! Inc., who will then compile the requested records at a time convenient to it, there exists

reasonable cause to permit the execution of the requested warrant at any time in the day or night.

69. Based on the information above, I have probable cause to believe that there exists evidence, fruits, instrumentalities, and/or contraband of as well as identity evidence of the perpetrator. By this affidavit and application, I request that the Court issue a search warrant directed to Yahoo! Inc. allowing agents to seize the e-mail and other information stored on the Yahoo! Inc.'s servers for the computer accounts and files identified in Attachments A and B.

70. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711(3) and 18 U.S.C. §§ 2703(a), (b)(l)(A) & (c)(l)(A). Specifically, the Court is "a district court of the United States ... that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(I).

71. Title 18 U.S.C. § 3238 provides, in relevant part, that jurisdiction for "[t]he trial of all offenses begun or committed ... out of the jurisdiction of any particular State or district, shall be in the district in which the offender, or any one of two or more joint offenders, ... is arrested or is first brought; but if such offender or offenders are not so arrested or brought into any district, an indictment or information may be filed in the district of the last known residence of the offender or of any one of two or more joint offenders ... , or if no such residence is known the indictment or information may be filed in the District of Columbia." The facts outlined above detail the methodology by which a group of individuals, primarily residing outside of the United States, engage in the sale and

distribution of receipt of child pornography. The email account listed in Attachment A has been used to arrange for the distribution of visual depictions of minors engaging in sexually explicit conduct into the United States, and the account is being accessed and controlled by individuals outside the United States. Therefore, the offenses detailed in this affidavit below are all offenses begun or committed out of the jurisdiction of any particular State of district. Furthermore, there is no last known residence for these offenders. Therefore, pursuant to 18 U.S.C. § 3238, this Court is the proper jurisdiction to issue the requested search warrant.

72. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Caliope Bletsis,
Special Agent
Federal Bureau of Investigation

Subscribed to and sworn before me this 14 day of November, 2014.

Signature

HONORABLE ALAN KAY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with:

NGETKO_22@YAHOO.COM I YAHOO ID: NGETKO_22

SEXY _LORRAINE05@YAHOO.COM /YAHOO ID: SEXY_ LORRAINE05

CUTIERHEA_l4@YAHOO.COM I YAHOO ID: CUTIERHEA_l4

MOUNTAINMAN007@YAHOO.COM I YAHOO ID: MOUNTAINMAN007

RL_1138@YAHOO.COM/YAHOO ID: RL_ll38

BARONWWl@Y AHOO.COM/ YAHOO ID: BARONWWI

Yahoo! email and messenger accounts that are stored at premises controlled by Yahoo! Inc., a company that accepts service of legal process at 701 First Avenue, Sunnyvale, California 94089.

ATTACHMENT B

Particular Things to be Seized and Procedures to Facilitate Execution of the Warrant

I. Information to be disclosed by Yahoo! (the "Provider") to facilitate execution of the warrant

To the extent that the information described in Attachment A is within the possession, custody, or control of Yahoo! Inc., including any emails, records, files, logs, or information that has been deleted but is still available to Yahoo! Inc., or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) October 7, 2014, Yahoo! Inc. is required to disclose the following information to the government for each account or identifier, including any information contained in that email account which is helpful to determine the account owner's true identity, listed in Attachment A:

a. The contents of all e-mails associated with the account, from the time of account creation to the present, including stored or preserved copies of e-mails sent to and from the account, e-mail attachments, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each email;

b. Any deleted emails, including any information described in subparagraph "a," above;

c. All records or other information regarding the identification of the account, to include full name,

physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. The types of service utilized;

e. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

f. All records pertaining to communications between Yahoo! Inc. and any person regarding the account, including contacts with support services and records of actions taken.

The Provider shall deliver the information set forth above via United States mail, courier, or e-mail to:

Caliope Bletsis
Federal Bureau of Investigations
Headquarters - Major Case Coordination Unit
801 International Drive
Linthicum, MD 21090
Caliope.Bletsis@ic.tbi.gov

II. Information to be seized by the government

1. All information described above in Section I, including correspondence, records, documents,

photographs, videos, electronic mail, chat logs, instant messages, and electronic messages, that constitutes fruits, evidence or instrumentalities of violations of 18 U.S.C. § 2251(a)(production of child pornography); 18 U.S.C. § 2252A(a)(2)(A), (b)(l) (receipt and distribution of child pornography); and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of child pornography) including, for each account or identifier listed on Attachment A, information pertaining to the following matters, including attempting and conspiring to engage in the following matters:

a. Any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct;

b. Any person knowingly persuading, inducing enticing, or coercing any individual who has not attained the age of 18 years, to engage in any sexual activity for which any person can be charged;

c. Any person knowingly transporting or receiving child pornography, as defined at 18 U.S.C. § 2256(8);

d. Any person knowingly transferring obscene matter to another individual who has not attained the age of 16 years, knowing that the other person has not attained the age of 16 years;

e. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

f. Identification of coconspirators, accomplices, and aiders and abettors in the commission of the above offenses;

g. Records relating to who created, used, or communicated with electronic account or identifier listed in Attachment A about matters relating to the criminal activity listed above, including identification of coconspirators, accomplices, and aiders and abettors in the commission of the above offenses, including records that help reveal their whereabouts.

2. Credit card and other financial information including, but not limited to, bills and payment information;

3. Evidence of who used, owned, or controlled the account or identifier listed on Attachment A, including evince of their whereabouts;

4. Evidence of the times the account or identifier listed on Attachment A was used;

5. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A and other associated accounts.

III. Government procedures for warrant execution

The United States government will conduct a search of the information produced by the Provider and determine which information is within the scope of the information to be seized specified in Section II That

information that is within the scope of Section II may be copied and retained by the United States.

Law enforcement personnel will then seal any information from the Provider that does not fall within the scope of Section II and will not further review the information absent an order of the Court.