ALANA W. ROBINSON
Acting United States Attorney
JENNIFER L. GMITRO
Assistant United States Attorney
California Bar Number 246797
Federal Office Building
880 Front Street, Room 6293
San Diego, California 92101-8893
Tel: (619) 546-9692
Jennifer.Gmitro@usdoj.gov
Attorneys for Plaintiff
United States of America

Attorneys for the United States

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. LUKE NOEL WILSON, Defendant	Case No.: 15CR2838-GPC **UNITED STATES' RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS** **Date: May 18, 2017** **Time: 1:30 p.m.** **Honorable Gonzalo P. Curiel**

Plaintiff, the UNITED STATES OF AMERICA, by and through its counsel, Alana W. Robinson, Acting United States Attorney, and Jennifer L. Gmitro, Assistant United States Attorney, hereby files its Response in Opposition to Defendant's Motion to Suppress. This response is based upon the files and records of the case, together with the included memorandum of points and authorities and the attached exhibits.

I.
STATEMENT OF THE CASE

On October 15, 2015, Defendant, Luke Noel Wilson, was arrested on a federal complaint charging him with distribution and possession of child pornography in

violation of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B). His initial appearance was held the following day. Defendant had counsel appointed and the government moved to detain Defendant.

On October 20, 2015, Defendant stipulated to being detained pending trial.[1] Defendant's retained counsel, Marc Kohnen, made his first appearance and relieved appointed counsel.

On November 10, 2015, a federal grand jury returned a three-count indictment charging Defendant with Advertising of Child Pornography in violation of 18 U.S.C. § 2251(d)(1)(A), Distribution of Child Pornography in violation of 18 U.S.C. § 2252(a)(2), and Possession of Child Pornography in violation of 18 U.S.C. § 2252(a)(4)(B). On November 12, 2015, Defendant was arraigned on the indictment and pleaded not guilty to the charges. The first Motion Hearing was set in this Court on December 18, 2015.

On December 14, 2015, at Defendant's request, the Motion Hearing was continued to February 5, 2016. This Court continued, at the joint request of the parties, the Motion Hearings which were set on March 18, 2016, April 22, 2016, June 10, 2016, and June 17, 2016.

On June 14, 2016, Defendant appeared before Magistrate Judge Jill Burkhardt and entered a plea of guilty to Count One of the Indictment, charging him with Advertising Child Pornography, pursuant to a plea agreement. A sentencing hearing was set for September 2, 2016. On June 15, 2016, the magistrate judge issued findings and made a recommendation that this Court accept Defendant's plea of guilty. On June 30, 2016, this Court accepted the guilty plea.

[1] Defendant requested a detention hearing which was held on December 15, 2015. After hearing the arguments of the parties, Magistrate Judge Jill L. Burkhardt set a $250,000 bond secured by two financially-responsible adults and requiring a $40,000 cash deposit. On May 11, 2017, Defendant's conditions of release were modified pending assessments and approval from pre-trial services. Defendant has not yet posted bond and remains in custody.

At the joint request of the parties, the sentencing hearing was continued from November 4, 2016 and was set for February 24, 2017.

On January 18, 2017, Defendant's second attorney filed his notice of appearance. On February 3, 2017, Defendant filed a Motion to Withdraw his Guilty Plea, and on March 17, 2017, Defendant filed a Supplemental Motion to Withdraw his Guilty Plea. On April 14, 2017, the Court granted Defendant's motion.

On April 28, 2017, Defendant filed his Motion to Suppress Evidence. An evidentiary hearing is set for May 18, 2017.

II.
STATEMENT OF FACTS

A. Internet Service Providers' Obligation to Report Child Pornography Under Title 18 U.S.C. § 2258A

Title 18 U.S.C. § 2258A mandates that if an Electronic Service Provider (ESP), "while engaged in providing an electronic communication service," obtains knowledge of facts and circumstances regarding apparent violations of federal statutes involving child pornography, such as 18 U.S.C. § 2252, it has a duty to report the information through the CyberTipline of the National Center for Missing and Exploited Children (NCMEC). 18 U.S.C. § 2258A(a). The ESP may include in the report information regarding the identity and location of the individual involved and "[a]ny image of apparent child pornography relating to the incident such report is regarding," including the "complete communication containing any image of apparent child pornography." 18 U.S.C. § 2258(b). NCMEC is then required to forward the report to an appropriate law enforcement agency. 18 U.S.C. (c)(1), (d)(2), and (g)(3). The Internet Crimes Against Children Task Force Program (ICAC program) is "a national network of 61 coordinated task forces" designed to engage in "both proactive and reactive investigations, forensic investigations, and criminal prosecutions," in response to "technology-facilitated child

sexual exploitation and Internet crimes against children," which includes the "online sharing of child sexual abuse images."[2]

B. Defendant's Agreement to Google's Terms of Service Upon Creation of e-mail Account soulrebelsd@gmail.com

On March 13, 2014, Defendant created the Google, Inc. (Google) e-mail account soulrebelsd@gmail.com. Exhibit ("Ex.") 1 (Google Subscriber Information for e-mail account soulrebelsd@gmail.com). At the time Defendant created the account, he agreed to Google's terms of service as of November 11, 2013.[3] On April 14, 2014, Google modified its Terms of Service, however relevant provisions regarding compliance with the law and Google's right to view content were not changed. See FN 3; Ex. 2 (Declaration of Cathy A. McGoff, Google, Inc. Senior Manager of Law Enforcement and Information Security and Attached Exhibit containing "Google Terms of Service") at 4-6. The Terms of Service stated, among other things, that Defendant may "use [Google] Services:

> only as permitted by law … [and Google] may suspend or stop providing our Services to you if you do not comply with our terms or policies or if we are investigating suspected misconduct.

Id. Google specifies that it:

> may review content to determine whether it is illegal or violates our policies, and we may remove or refuse to display content that we reasonably believe violates our policies or the law.

Id. The Terms of Service also state that Google may:

> modify these terms or any addition terms that apply to a Service to, for example, reflect changes to the law or changes to our Services. You should

---

[2] https://www.ojjdp.gov/programs/ProgSummary.asp?pi=3

[3] Google makes its current and past versions of its Terms of Service available http://www.google.com/intl/en/policies/terms/archive/, which contains a link to Google's November 11, 2013 Terms of Services. The following is a direct link to those terms: http://www.google.com/intl/en/policies/terms/archive/20131111/.

> look at the terms regularly. We'll post notice of modifications to these terms on this page. …. If you do not agree to the modified terms for a Service, you should discontinue your use of that Service.

Id.

With respect to its terms of service and with regard to child pornography material in particular, Google maintains:

> Google has a strong business interest in enforcing our terms of service and ensuring that our products are free of illegal content, and in particular, child sexual abuse material. We independently and voluntarily take steps to monitor and safeguard our platform. If our product is associated with being a haven for abusive content and conduct, users will stop using our services. Ridding our products and services of child abuse images is critically important to protecting our users, our product, our brand, and our business interests.

Ex. 2 at 1 (¶ 3).

C. Google's Methods of Reviewing Accounts for Child Pornography

"Based on [its] private, non-government interest, since 2008, Google has been using its own proprietary hashing technology to tag confirmed child sexual abuse images" uploaded by users of its Service. Ex. 2 at 1 (¶ 4). Essentially, Google employees view and confirm that an image contains child pornography as defined by 18 U.S.C. § 2256, then assign a "hash" value, or "digital fingerprint," to the image, which can then be used to search user accounts for duplicate images. Id. at 1-2 (¶¶ 4-7).

D. Google's Identification of Child Pornography in Defendant's Account and The NCMEC CyberTip

On or about June 17, 2015, the National Center for Missing and Exploited Children (NCMEC) provided a CyberTipline report[4] to the San Diego ICAC Task Force. Ex. 3

[4] In March 1998, NCMEC launched the CyberTipline to further NCMEC's mission of helping to prevent and diminish the sexual exploitation of children. The CyberTipline provides the public and electronic service providers (ESPs) with the ability to report online (and via toll-free telephone) instances of online enticement of children for sexual acts, extra-familial child sexual molestation, child pornography, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names,

(CyberTip Report). The report indicated that Google became aware of four image files depicting suspected child pornography which were uploaded to an email on June 4, 2015, by an individual using email address soulrebelsd@gmail.com, Defendant's e-mail account. Id. at 3, 9-11.

As set forth in the report, Google classified the four images as Child Pornography category "A1," meaning that the images depicted a prepubescent minor, signified by the "A," engaged in a sexual act, signified by the "1" (as opposed to a pubescent minor ("B"), or a lascivious exhibition ("2")). Id. at 12; see also Ex. 2 at 2 (¶ 9) (A1 classification indicates the image depicted a "prepubescent minor engaged in a sexual act."). Google had identified the four images as child pornography based on its proprietary hashing technology, described in Section II.C., above. That is, a Google employee had previously viewed the images, determined that they were child pornography, created a unique "hash" value, or "digital fingerprint," and thereby identified duplicates of the previously identified child pornography images uploaded to Defendant's e-mail account. See Ex. 2 at 1-2 (¶¶ 4-7). Google terminated service for Defendant's e-mail account the same day, June 4, 2015. Ex. 1.

The four images were attached to the CyberTip report. The CyberTip report, while classifying the images as depicting a prepubescent minor engaged in a sex act, did not state whether a Google employee had or had not opened and physically viewed the specific attachments/images uploaded in Defendant's e-mail. Ex. 3. The CyberTip Report did indicate that NCMEC had not viewed the images:

> Please be advised that NCMEC has not opened or viewed any uploaded files submitted with this report and has no information concerning the content of the uploaded files other than information provided in the report by the ESP.

---

and misleading words or digital images on the Internet. NCMEC continuously reviews CyberTipline reports to ensure that reports of children who may be in imminent danger get first priority. After NCMEC's review is completed, all information in a CyberTipline report is made available to law enforcement.

Ex. 3 at 16.

In addition to the files depicting suspected child pornography, Google provided recent login information associated with the soulrebelsd@gmail.com account, including logins from a device(s) possessing Internet protocol (IP) address 99.113.198.241 on June 4, 2015, at 15:07:19 Universal Time Coordinated (UTC) and on May 9, 2015, at 15:48:04 UTC. Id. at 4-10. Google also identified jameskindle2012@gmail.com as a secondary email address associated with the soulrebelsd@gmail.com account. Id. at 10.

Once ICAC printed the report and the four attached images, the printed report and images were given to Homeland Security Investigation (HSI) Special Agent (SA) William Thompson, to handle the investigation. SA Thompson reviewed the report and the four images, and determined they depict child pornography. The following are descriptions of each of these four images with their file names and associated upload dates and times as identified by Google:

1. 140005125216.jpg: This image depicts a prepubescent female who is lying on her stomach with her face in the genital region of an older female who is seated with her legs spread. A second prepubescent female is also visible in this image and she is partially nude with her vagina exposed.

2. 140005183260.jpg: This image depicts a prepubescent female who is lying on top of another female. Within this image, the genital regions of the prepubescent female and female are pressed against one another and the older girl appears to be touching the face of the younger child with her tongue.

3. 140005129034.jpg: This image depicts a prepubescent female who is lying on her back with her legs spread and her vagina exposed. An older female is positioned in front of this girl's exposed vagina in this image and the younger girl has her left hand on the vaginal/buttocks area of a second nude girl of similar age.

4. 140005200787.jpg: This image depicts a wider angle view of the previously referenced images possessing file names 140005125216.jpg and 140005129034.jpg.

E. Follow-Up Investigation and Search Warrants

1. Subscriber Information

On July 6, 2015, SA Thompson submitted a Department of Homeland Security (DHS) Summons to Google requesting subscriber information for email accounts soulrebelsd@gmail.com and jameskindle2012@gmail.com. Google responded and provided the following information in summary:

> soulrebelsd@gmail.com:
> Name: Luke W
> Creation Date: 03/13/2014
> Recovery e-Mail: jameskindle2012@gmail.com
>
> jameskindle2012@gmail.com:
> Name: James Kindle
> Creation Date: 01/13/2012
> Short Messaging Service (SMS) #: 16198867825

SA Thompson also submitted a DHS Summons to AT&T Internet Services requesting subscriber information for IP address 99.113.198.241 on June 4, 2015 at 15:07:19 UTC and May 9, 2015 at 15:48:04 UTC. AT&T Internet Services responded. and provided the following information in summary:

> Name: Luke WILSON
> Address: 6540 Reflection Drive, Apartment 1306, San Diego, CA 92124
> Established Date: 08/18/2014
> Cell Phone: ending in 7825

2. Search Warrant for Defendant's Google E-mail Account soulrebelsd@gmail.com

On July 29, 2015, SA Thompson obtained a state search warrant for the soulrebelsd@gmail.com email account. Ex. 4. Probable cause for the warrant was based upon the tip provided by Google and SA Thompson's review of the four images, identified in Section II.D., above. Id. 4-8. In the Probable Cause section, SA Thompson nowhere indicated that he had obtained a search warrant before reviewing the four images. Id.

Prior to bringing the warrant application to the judge for review, SA Thompson consulted with a Deputy District Attorney. Id. at 8.

Upon review of the data produced by Google from the soulrebelsd@gmail.com account, SA Thompson located dominion and control emails linking Defendant to the account. Specifically, purchase order receipts and invoices containing Defendant's name and residential address.

Additional review of this search warrant results revealed email exchanges between Defendant, using email address soulrebelsd@gmail.com, and other individuals. For example, the results provided by Google revealed the following:

(1) An email sent from jenalynarriolax3@gmail.com to soulrebelsd@gmail.com on July 17, 2014, which reads "Sent from my iPhone" and attaches a video entitled "Video.MOV." "Video.MOV" is a video approximately forty-five seconds in length which depicts a young, prepubescent child lying on top of and facing an adult female who pulls the prepubescent child's underwear down, touches the child's buttocks, and pulls them apart to expose the child's anus.

(2) An email sent from soulrebelsd@gmail.com to jenalynarriolax3@gmail.com on September 1, 2014, evidencing Defendant's violation of 18 U.S.C. § 2251(d)(1)(A) (Advertising of Child Pornography):

> "yes i can -but what do I owe you for 3 pictures - the deal I sent was:
>
> i will pay $150
>
> 3 minute video of you with the [female child] sleeping on your chest or lap ... well you either pull up your skirt/or take pants and panties off – and play with your pussy - need you to show the girl, your face, and fingers going inside you.
>
> would be awesome if she is asleep on your lap with her face just above your pussy (;
>
> will pay $50 more if you do video of you fingering yourself and get finger super wet then slowly slide finger on the girls lips (=

> will pay $50 more if you get pic of her pussy wide open with face showing (=
>
> thanks!"

(3) An email sent from soulrebelsd@gmail.com to jenalynarriolax3@gmail.com on February 5, 2015, with the subject "Re: Game plan," reading:

> 1. pics and vid of the [female child] (would pay $200) or
> 2. Pics and vid of you and [another female child] (would pay $200)
> 3. A freaky chat (pay $60)
> 4. A video shoot of us doing freaky stuff … pending what your down to do! I always wanted to play withyou after your man had cummed inside you earlier in the day!"

On Febraury 7, 2015, jenalynarriolax3@gmail.com responded, "I'll do number 2 later."

(4) An email sent from soulrebelsd@gmail.com to jenalynarriolax3@gmail.com on May 12, 2015, with the subject "hey…," reading: "I will drop you $250 cash if you do a total of 3 minutes of videos of you and [a female child] kinda like before…I can give you step by step directions so its just you basically acting. (=."

SA Thompson also located emails with child pornographic file attachments he sent to an individual other than Arriola, which contained eighteen image file attachments. Seventeen of the attachments contain child pornography images. Two of the images are described below:

(1) Adry_MS_N_2.jpg – This image depicts a nude prepubescent girl who is lying on her back with her legs raised toward her chest exposing her vagina and anus.

(2) AdryPlayWithDelyandDad(2).jpg – This image depicts a nude prepubescent girl who is positioned in front of and holding an adult male's penis.

//
//
//
//

3. Search Warrant for Defendant's Residence

On August 17, 2015, law enforcement obtained a state search warrant for Defendant's residence. Ex. 5. Probable cause for the warrant was based upon the CyberTip report containing the information provided by Google, SA Thompson's review of the four images described in Section II.D., above, subscriber and other information provided by Internet Service Providers, database and law enforcement queries, and physical surveillance conducted at Defendant's residence. Id. at 7-12. In the Probable Cause section, SA Thompson nowhere indicated that he had obtained a search warrant before reviewing the four images. Id. at 7-9. Prior to bringing the warrant application to the judge for review, SA Thompson consulted with a Deputy District Attorney. Id. at 12.

The warrant was executed the next day, and law enforcement seized multiple electronic devices. During execution of the warrant, after securing the residence, a San Diego Police Department (SDPD) officer who was positioned on perimeter security notified investigators he observed a black and green Monster Energy backpack being tossed over Defendant's third floor balcony at the same time he heard loud knocking at one of the upper apartments, which corresponded to the knock and notice upon Defendant's residence door. Upon entry into the apartment, Defendant was located in the residence.

SA Thompson conducted a cursory search of the black and green Monster Energy backpack and discovered Defendant's Bank of America check book and a SanDisk 64 gigabyte (GB) thumb drive. During an on scene forensic preview of the SanDisk 64 GB thumb drive, SA Thompson discovered thousands of child pornography images primarily depicting prepubescent girls, approximately five to ten years of age, involved in sexual activity, including the four images reported by Google to NCMEC, described in Section II.D., above.

//

//

//

4. Follow-up Investigation of Arriola

Subscriber and other information related to the Google account for jenalynarriolax3@gmail.com identify Jenalyn Arriola as the individual who utilizes that account. Law enforcement subsequently located Arriola.

On August 20, 2015, SA Thompson advised Jenalyn Arriola of her Miranda rights, which she waived, agreeing to make a statement. Arriola admitted to molesting two minor females and to producing child pornography depicting these molestations, including the video entitled "Video.MOV," described in Section II.E.2.(1), above, which she sent to Defendant upon his request and in return for monetary payment. Arriola stated that she sent child pornography images and videos to Defendant primarily via email and text message, and identified her email accounts, including jenalynarriolax3@gmail.com, and Defendant's email account, soulrebelsd@gmail.com.

On August 31, 2015, SA Thompson obtained a search warrant for various Google accounts belonging to Arriola, including jenalynarriolax3@gmail.com. Ex. 6. Probable cause for the warrant was based on information obtained from the results of the warrant executed on Defendant's e-mail account, including email exchanges in which Defendant and Arriola discuss the production of child pornography and Arriola sends Defendant the video "Video.MOV" depicting child pornography, as well as Arriola's admissions made on August 20, 2015. Id. at 4-8. SA Thompson specified in the Probable Cause statement that he had previously obtained a warrant for Defendant's e-mail account. Id. Prior to bringing the warrant application to the judge for review, SA Thompson consulted with a Deputy District Attorney. Id. at 8.

On September 8, 2015, Google responded to the search warrant, producing from the jenalynarriolax3@gmail.com e-mail account multiple email exchanges between Defendant and Arriola evidencing Defendant's violations of 18 U.S.C. § 2251(d)(1)(A), as well as Defendant's possession and receipt of child pornography, including the September 1, 2014 email set forth in Section II.E.2.(2), above.

III.
ARGUMENT

A. The Agent's Visual Viewing of the Four Images Did Not Exceed the Scope of Google's Private Search

The Fourth Amendment "proscrib[es] only governmental action" and therefore "it is wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government." United States v. Jacobson, 466 U.S. 109, 113 (1984) (citations omitted). The Fourth Amendment "does not prohibit governmental use of [] information" found when a private party conducts a search. Id. at 117. Accordingly, when a government agent reviews information provided by a private party, or conducts another search based on that information, any "additional invasions of… privacy by the government agent must be tested by the degree to which they exceed[] the scope of the private search." Id. at 115. The reasonableness of the government's action is "appraised on the basis of the facts as they existed at the time that invasion occurred." Id. When the information provided by a private party makes it a "virtual certainty that nothing else of significance" will be discovered by the government agent that was not already discovered by the private party, there is no Fourth Amendment violation. Id. at 119.

In Jacobson, Federal Express employees identified a damaged package (a cardboard box wrapped in brown paper) and, pursuant to the company's policy regarding insurance claims, further examined the contents of the package, and eventually notified the Drug Enforcement Administration (DEA) who arrived and conducted a field test on the substance, determining that it was cocaine. Jacobson, 466 U.S. at 111. The Supreme Court held that any "additional invasions of [the defendant's] privacy by the government agent must be tested by the degree to which they exceeded the scope of the private search." Id. at 115. The Court found that the DEA agents' removal of the tube, bags, and powder from the box, as well as the chemical field test, were reasonable and did not violate the Fourth Amendment. Id. at 118. Even though the private party had not

conducted a chemical field test on the substance, the Court determined that when the DEA conducted the chemical test, it did not expand the private party search. Id. at 122-23. The Court noted, "[it] is probably safe to assume that virtually all of the tests conducted under circumstances comparable to those disclosed by this record would result in a positive finding; in such cases, no legitimate interest has been compromised." Id. at 123. There was a "virtual certainty that nothing else of significance" would be revealed by the government's search. Id. at 119.

Here, the private party search conducted by Google went even further than the private party search in Jacobson, because Google already conducted its own "field test" on the four images, determining with a "virtual certainty" that they constituted child pornography. See id. at 119. This is true because a Google employee had already viewed the images and determined they constituted images of prepubescent minors engaged in a sexual act pursuant to 18 U.S.C. § 2256, created a unique "hash," or "digital fingerprint," for the images, and then identified the identical, duplicate images uploaded to Defendant's e-mail account. Hash values are, "essentially 'digital fingerprint[s]' … [which] remain unchanged as long as the file itself is not altered." United States v. Dreyer, 804 F.3d 1266, 1270 (9th Cir. 2015). It is "safe to assume that virtually all" images identified as having hash values that match up with known child pornography will result in a "positive finding" of child pornography, and therefore no additional legitimate privacy interest has been compromised. See Jacobson, 466 U.S. at 123. Indeed, Google specified that the images depicted a "prepubescent minor" engaged in a "sexual act." Law enforcement's viewing of the images – after it received the CyberTipline report from NCMEC – did not constitute an expansion of Google's search, and the evidence should not be suppressed.

B. Even if There Were a Fourth Amendment Violation, the Evidence Should Not be Suppressed Because the Special Agent Acted in Good Faith

Even if the Court finds that viewing the four images violated Fourth Amendment protections, the evidence should not be excluded. "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and

sufficiently culpable that such deterrence is worth the price paid by the justice system." Herring v. United States, 555 U.S. 135, 140-41 (2009). As set forth below, under these circumstances, suppression of the evidence would not serve the exclusionary rule's "sole purpose," which is "to deter future Fourth Amendment violations." Davis v. United States, 564 U.S. 229, 236-37 (2011) (citations omitted).

Neither the ICAC team nor SA Thompson demonstrated a deliberate, reckless, or grossly negligent disregard for Defendant's Fourth Amendment rights in this matter, but acted based on a good faith belief that a search warrant was not required. Indeed, the four images Google identified had been forwarded to ICAC, as required by 18 U.S.C. 2258A, through the CyberTipline. In his affidavit in support of the search warrant for Defendant's e-mail account and residence, SA Thompson made no misrepresentations, and Defendant makes no such allegation. SA Thompson specified in his Probable Cause statement that Google had provided "suspected" images of child pornography, which SA Thompson then reviewed. Ex. 4 at 4-8; Ex. 5 at 7-12. SA Thompson had not obtained a warrant to view the images and did not represent that he obtained a warrant to view the images. Id.[5] His candor is evident when the affidavits for the search warrants on Defendant's e-mail and residence (Ex.s 4 & 5) are compared to the affidavit submitted for the search warrant on Arriola's e-mail account (Ex. 6). When SA Thompson applied for a search warrant for Arriola's e-mail account, he set forth facts in support of probable cause, clearly stating in his affidavit that such facts were based on information obtained as a result of the execution of the warrants on Defendant's e-mail account. Ex. 6 at 4-5 (describing e-mail content after stating that the content had been obtained pursuant to "search warrant service" based on the July 29, 2015 search warrant number 49815 signed by a San Diego Superior Court Judge). Importantly, SA Thompson reviewed all of the search warrants

[5] Additionally, there was no information readily apparent on the face of the CyberTipline report indicating that the contents had not been previously reviewed. And because of Google's method of identifying child pornography via its repository of known child pornography images, the images had in effect been previously viewed.

for legal sufficiency with a Deputy District Attorney before presenting them to a judge. Ex. 4 at 8; Ex. 5 at 12; Ex. 6 at 8 (all stating that the affidavit was reviewed by a Deputy District Attorney for legal sufficiency). Such consultation is of "significant important to a finding of good faith." United States v. Winsor, 549 Fed. Appx. 630, 632 (9th Cir. 2013) (quoting United States v. Brown, 951 F.2d 999, 1005 (9th Cir. 1992)). Law enforcement viewed the four Google images, and obtained subsequent search warrants based on these images, all in good faith, and suppression would therefore fail to deter future Fourth Amendment violations.

Furthermore, SA Thompson acted "in objectively reasonable reliance" on the warrants. See United States v. Leon, 468 U.S. 897 (1984). Defendant does not contend that SA Thompson misled the magistrate or that the magistrate improperly issued the warrant, and the record would not support such a finding. Even so, "'[g]reat deference' should be given to a magistrate judge's determination and "resolution of doubtful or marginal cases in this area should largely be determined by the preference to be accorded to the warrants." Kelley, 482 F.3d at 1050-51. Accordingly, SA Thompson's execution of the subsequent e-mail and residential search warrants was "objectively reasonable" and the evidence obtained as a result should not be suppressed. Leon, 468 U.S. at 913-925.

Because SA Thompson was acting in good faith, suppression would not serve the purpose of deterring future Fourth Amendment violations. See Davis, 564 U.S. at 236-37. On the contrary, the "price paid by the justice system" would be significant. See Herring, 555 U.S. at 140-41. To suppress the evidence would exclude "reliable, trustworthy evidence bearing on [Defendant's] guilt or innocence," Davis, 564 U.S. at 237, regarding a crime that constitutes "'a serious national problem.'" Paroline v. United States, 134 S. Ct. 1710, 1716 (2014) (quoting New York v. Ferber, 458 U.S. 747, 749 (1982)).

C. Not All Evidence Constitues "Fruit of the Poisonous Tree"

Defendant seeks to suppress "all the evidence in this case." Def.'s Mot. at 21-22. But not all evidence in this case constitutes fruit of the poisonous tree.

First, even if the Court found a Fourth Amendment violation as to the four images that were the basis for the subsequent search warrant into Defendant's e-mail account and residence, "[t]he mere inclusion of tainted evidence in an affidavit does not, by itself, taint the warrant or the evidence seized pursuant to the warrant." United States v. Vasey, 834 F.2d 782, 788 (9th Cir. 1987) (citation omitted)). This is because, even if the purportedly tainted evidence were excised, "the remaining, untainted evidence would provide a neutral magistrate with probable cause to issue a warrant." Id. A magistrate judge may issue a warrant if there is a "fair probability that contraband or evidence" of a crime will be found at the location to be searched and "[n]either certainty nor a preponderance of the evidence is required." United States v. Kelley, 483 F.3d 1047, 1050 (9th Cir. 2007).

Here, a magistrate may have determined that the affidavits established probable cause existed even without the description of the four images. In United States v. Patrick, 365 Fed. Appx. 834 (9th Cir. 2010) (unpublished), the Ninth Circuit upheld a search warrant based on a "citizen informant['s]" representation to law enforcement that he had seen "pornographic pictures of children involved in sexual acts" on the defendant's computer, with no additional description other than that they were "very young girls." Id. at 836. Because the informant had no motive to lie, and could have been prosecuted if he had been untruthful, the information was determined to be reliable. Id. The same circumstances are present here, where Google informed law enforcement that it had discovered images of child pornography in Defendant's e-mail account. Given Google's familiarity with child pornography – based on a repository of ***known*** child pornography images – and its obligation under the law to report such images to law enforcement, a magistrate could have found there was probable cause to search Defendant's e-mail account in the absence of the four images. See id.; see also United States v. Smith, 795 F.3d 841 (9th Cir. 1986) (upholding warrant where affidavit stated an "experienced postal inspector" had seen photos depicting "three juvenile girls engaged in 'explicit sexual conduct,'" with no additional description); United States v. Thomas, 788 F.3d 345, 348-49, n.5, 353-353 (2d Cir. 2015) (upholding search warrant where detective did not view

offending files that were the basis for the warrant, but compared the "hash values – or the 'digital fingerprints' – of the defendant's files with the hash values of images known to be child pornography").

Additionally, as set forth herein, SA Thompson subsequently obtained search warrants for other individuals' e-mail accounts and residences. "It has long been the rule that a defendant can urge the suppression of evidence obtained in violation of the Fourth Amendment only if that defendant demonstrates that his Fourth Amendment rights were violated by the challenged search or seizure." United States v. Padilla, 508 U.S. 77, 81 (1993). "A person who is aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by a search of a third person's premises or property has not had any of his Fourth Amendment rights infringed" and lacks standing to challenge the introduction of the evidence obtained as a result of the search. Rakas v. Illinois, 439 U.S. 128, 134 (1978). Additionally, where, for example, Ms. Arriola admitted to law enforcement that she had sent and received communications about and images and/or videos of child pornography with Defendant, there was adequate probable cause to obtain a search warrant for her e-mail account. See Ex. 6.

Finally, when Defendant threw his backpack containing a thumb drive depicting thousands of child pornography onto the ground when law enforcement arrived and knocked at his residence, he abandoned his property interest in that bag and its contents. Defendants actions where an objective indication that he "relinquished a reasonable expectation of privacy in the property." United States v. Nording, 804 F.2d 1466, 1469 (9th Cir. 1986). Accordingly, the contents should not be suppressed. See id. at 1470 (leaving a tote bag on an airplane where anyone could access it supports an inference that the defendant intended to abandon the bag); United States v. Juszczyk, 844 F.3d 1213 (10th Cir. 2017) (no objectively reasonable expectation of privacy when defendant abandoned his backpack by throwing it onto someone else's roof to conceal it from police); United States v. Hardy, 543 Fed. Appx. 721, 722 (9th Cir. 2013) (defendant abandoned backpack by denying ownership); United States v. Hinsey, 414 Fed. Appx.

983, 985 (9th Cir. 2011) (abandonment does not require both verbal and physical relinquishment);

D. Defendant Has Not Establish That He Had a Reasonable Expectation of Privacy

Finally, even if the Court finds that law enforcement's review of the four images exceeded the scope of Google's private party search, Defendant still has not met his burden of demonstrating that, at the time law enforcement viewed the images, (1) Defendant had an actual, subjective expectation of privacy in the images; and (2) society is prepared to recognize that expectation as objectively reasonable. United States v. Nerber, 222 F.3d 597, 599 (9th Cir. 2000). The validity of any privacy expectation depends "entirely on its context." United States v. Ziegler, 474 F.3d 1184, 1188-89 (9th Cir. 2007) (citation omitted).

Defendant nowhere explains how he had a subjective expectation of privacy when Google's terms explicitly state that its Services may not be used to violate the law and that Google may "review content" to determine whether it is "illegal." Even if Defendant were able to establish he had a subjective expectation of privacy before Google terminated his account, demonstrating such an expectation ***after*** the account's termination is another matter. Defendant has not established that such an expectation is one that society is prepared to recognize as objectively reasonable. Here, Google had exercised its right to monitor its system, identified child pornography in Defendant's e-mail account, and terminated the account, turning the images over to NCMEC as it was required to by law. Defendant could not have had a reasonable expectation of privacy in his account at this point. [6]

---

[6] Evaluating a subjective or objectively reasonable privacy expectation depends on the context. In this case, the ESP is required to report specific, illegal content – child pornography. In In re Grand Jury Subpoena, JK-15-029, 828 F.3d 1083 (9th Cir. 2016), the Ninth Circuit held that an individual who was a government official did not have a reasonable expectation of privacy as to private e-mails relating to his official business, because the state public records laws granted the public a right to inspect "any writing

Courts considering whether an expectation of privacy is objectively reasonable look sources "outside the Fourth Amendment, such as concepts of real or personal property law or to understandings that are recognized and permitted by society." Rakas v. Illinois, 439 U.S. 128, 143-44 (1978). None of these concepts support an expectation of privacy here. See e.g., United States v. Cunag, 386 F.3d 888, 895 (9th Cir. 2004) (defendant did not have an expectation of privacy in a hotel room after the hotel took "affirmative steps" to evict him); United States v. Bautista, 362 F.3d 584, 590 (9th Cir. 2004) (whether defendant had a reasonable expectation of privacy in a hotel room depends on whether the hotel "justifiably terminated [the defendant's' control of the room through private acts of dominion"). Google had terminated Defendant's rights to access the account, and Defendant has not established a legitimate expectation that its contents would be kept private.

IV.

CONCLUSION

For the reasons set forth herein, the United States requests that the Court deny Defendant's Motion to Suppress Statements, except where unopposed.

DATED: May 11, 2017

Respectfully Submitted,
ALANA W. ROBINSON
Acting United States Attorney

/s/ Jennifer L. Gmitro
JENNIFER L. GMITRO
Assistant U.S. Attorney

---

that contains information relating to the conduct of the public's business." Id. at 1089-91. In other words, the content of the communication was important to determining whether the official had a reasonable expectation of privacy. This reasoning is applicable here. While Defendant may have a reasonable expectation that his e-mail account will generally remain private, it is not reasonable to expect such privacy when the e-mail communications contain child pornography, the ESP has terminated his access to the account, and the ESP was required by law to make the report.

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,

Plaintiff,

v.

LUKE NOEL WILSON,

Defendant.

Case No. 15CR2838-GPC

CERTIFICATE OF SERVICE

IT IS HEREBY CERTIFIED THAT:

I, Jennifer L. Gmitro, am a citizen of the United States and am at least eighteen years of age. My business address is 880 Front Street, Room 6293, San Diego, California 92101-8893.

I am not a party to the above-entitled action. I have caused service of the United States' Response in Opposition to Defendant's Motion to Suppress and this Certificate of Service on the following parties by electronically filing the foregoing with the Clerk of the District Court using its ECF System, which electronically notifies them:

John Kirby, Esq.,

Attorneys for Defendant

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

Executed on May 11, 2017.

Respectfully Submitted,

/s/ Jennifer L. Gmitro
JENNIFER L. GMITRO
Assistant U.S. Attorney