UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. LUKE NOEL WILSON, Defendant.	Case No.: 3:15-cr-02838-GPC **ORDER DENYING DEFENDANT'S MOTION TO SUPPRESS** **[ECF No. 57.]**

Before the Court is Defendant Luke Noel Wilson's ("Defendant's" or "Wilson's") Motion to Suppress Evidence as a Result of an Illegal Search. (Dkt. No. 57.) The motion has been fully briefed. (Dkt. Nos. 62, 65.) The Court conducted an evidentiary hearing and took the matter under submission on May 18, 2017. (Dkt. No. 67.) Upon consideration of the moving papers, applicable law, and argument of counsel, and for the reasons set forth below, the Court **DENIES** Defendant's motion to suppress.

BACKGROUND

A. Factual Background

1. Google, Inc. ("Google") Has a Statutory Duty to Report Known Child Pornography Violations.

Google is mandated by law to report known child pornography violations to the CyberTipline of the National Center for Missing and Exploited Children ("NCMEC").

18 U.S.C. 2258A(a) mandates that Internet service providers ("ISPs") that "obtain[] actual knowledge of any facts or circumstances" evincing "apparent" child pornography violations must submit, "as soon as reasonably possible," reports to the CyberTipline.[1] 18 U.S.C. § 2258A(a). An ISP may include in the report information about the identity and geographic location of the individual involved; historical reference information regarding the uploading, transmittal, or receipt of the apparent child pornography, or regarding the circumstances of the ISP's discovery of the apparent child pornography; any image of apparent child pornography relating to the incident in the report; as well as "[t]he complete communication containing any image of apparent child pornography." *Id.* § 2258A(b). ISPs that "knowingly and willfully" fail to make a report to the CyberTipline face financial sanctions. *See id.* § 2258A(e). The statute requires NCMEC to forward each report it receives to federal law enforcement agencies and permits NCMEC to forward the reports to state and local law enforcement. *See id.* § 2258A(c).

2. Google's Proactively Screens for Child Pornography to Further its Private Business Interests.

To further its private business interests, Google takes proactive measures beyond what is statutorily mandated by 18 U.S.C. § 2258A to screen for, report, and remove child pornography from its products and services. (*See* Dkt. No. 62-2, Declaration of Cathy A. McGoff ("McGoff Decl.").)

> 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. . . . Ridding our products and services of child abuse images is critically important to protecting our users, our product, our brand, and our business interests.

(*Id.* ¶ 3.)

[1] ISPs are "electronic communication service providers" ("ESPs"). *See generally* 18 U.S.C. § 2258A.

Google identifies and removes child pornography by employing a process that involves both visual inspection by trained employees and technological screening by Google's proprietary "hashing" technology. Google has been using its own hashing technology to identify child pornography since 2008. (*Id.* ¶ 4.) The process is as follows. First, Google trains a team of employees on Google's statutory duty to report apparent child pornography. (*Id.* ¶ 6.) This team is further "trained by counsel on the federal statutory definition of child pornography and how to recognize it on [Google's] products and services." (*Id.*)

Second, offending images are catalogued and assigned "hash values," which are often described as "digital fingerprints."[2] Specifically,

> Each offending image, after it is viewed by at least one Google employee, is given a digital fingerprint ("hash") that our computers can automatically recognize and is added to our repository of hashes of apparent child pornography as defined in 18 USC § 2256. Comparing these hashes to hashes of content uploaded to our services allows us to identify duplicate images of apparent child pornography to prevent them from continuing to circulate on our products.

(*Id.* ¶ 4 (emphasis added).)[3]

Third, Google's system searches its products and services for hash values that match hash values in its repository of known child pornography images.

> When Google's product abuse detection system encounters a hash that matches a hash of a known child sexual abuse image, in some cases Google automatically reports the user to NCMEC without re-reviewing the image. In other cases,

[2] "A hash value is (usually) a short string of characters generated from a much larger string of data (say, an electronic image) using an algorithm—and calculated in a way that makes it highly unlikely another set of data will produce the same value." *United States v. Ackerman*, 831 F.3d 1292, 1294 (10th Cir. 2016) (Gorsuch, J.), *reh'g denied* (Oct. 4, 2016) (citing Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38, 38–40 (2005)).

[3] Google "also rel[ies] on users who flag suspicious content they encounter so [Google] can review it and help expand [its] database of illegal images." (Dkt. No. 62-2, McGoff Decl. ¶ 5.) These user-flagged images must nonetheless be reviewed by a trained Google employee before being added to the hash repository. Google makes clear that "[n]o hash is added to [its] repository without the corresponding image first having been visually confirmed by a Google employee to be apparent child pornography." (*Id.*)

> Google undertakes a manual, human review, to confirm that the image contains apparent child pornography before reporting it to NCMEC.

(*Id.* ¶ 7.) Finally, Google provides a CyberTipline Report to NCMEC. (*Id.* ¶ 8.)

As a result of this multi-tiered process, Google's proprietary hashing technology "tag[s] *confirmed* child sexual abuse images" that are "*duplicate* images of apparent child pornography" previously identified by at least one trained Google employee. (*Id.* ¶ 4 (emphasis added).)

3. Defendant Agreed to Google's Terms of Service and Created a Google Email Account.

On March 13, 2014, Defendant created a Google email account with the username soulrebelsd@gmail.com. (Dkt. No. 62-1 at 2, Ex. 1.) Defendant agreed to Google's November 11, 2013 Terms of Service upon creation of the account. (Dkt. No. 62 at 4.) On April 14, 2014, Google modified its Terms of Service. (Dkt. No. 62-2 at 5–7, McGoff Decl. Ex. A.)[4] The April 14, 2014 Terms of Service contained the following provisions, in relevant part.

Google instructed users: "You may use our Services only as permitted by law," and "[w]e 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." (Dkt. No. 62-2 at 5, McGoff Decl. Ex. A.)

Regarding user content, Google stated,

> We 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. But that does not necessarily mean that we review content, so please don't assume that we do.

(*Id.*)

[4] The April 14, 2014 Terms of Service informed users that "[b]y using our Services, you are agreeing to these terms." (Dkt. No. 62-2 at 5, McGoff Decl. Ex. A.) Defendant continued using Google's Services and thus agreed to the April 14, 2014 Terms of Service.

Google notified users, "Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored." (*Id.*)

Finally, Google reminded users that Google

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

4. Google Identified Four Confirmed Child Pornography Images in Defendant's Email and Provided a CyberTipline Report to NCMEC.

On June 4, 2015, Google, by way of its proprietary hashing technology, became aware that Defendant uploaded four image files depicting child pornography to an email in his Google account. (Dkt. No. 62-3 at 4, 11–13, Ex. 3.) Google complied with its legal obligation under 18 U.S.C. § 2258A and provided a CyberTipline Report to NCMEC. (*Id.*) Defendant's email account was terminated on June 4, 2015. (Dkt. No. 62-2, McGoff Decl. ¶ 9; Dkt. No. 62-1 at 2.)

On June 5, 2015, NCMEC received CyberTipline Report # 5074778 from Google. (Dkt. No. 62-3, Ex. 3.) The report included information about the date and time Defendant uploaded the four child pornography images, the email address soulrebelsd@gmail.com and recent login information associated with the account (including logins from a device possessing Internet protocol ("IP") address 99.113.198.241 on June 4, 2015 at 15:07:19 UTC and on May 9, 2015 at 15:48:04 UTC), and the secondary email address associated with the soulrebelsd@gmail.com account, jameskindle2012@gmail.com. (*Id.*) The report also included the four image files, each of which Google classified as "A1" in accordance with the industry classification

standard. (*Id.*; *see also* Dkt. No. 62-2, McGoff Decl. ¶¶ 9–11.) "A1," in short, indicates that the file content contains a depiction of a prepubescent minor engaged in a sex act. (*Id.*)

Specifically, "A" signifies "Prepubescent Minor," whereas "B" signifies "Pubescent Minor." (Dkt. No. 62-3 at 14, Ex. 3.) "1" denotes "Sex Act," defined as: "Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value." (*Id.*) "2" denotes "Lascivious Exhibition," defined as: "Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value." (*Id.*)

Google did not forward the email itself to NCMEC. The report did not include any email body text or header information associated with the reported offending content. (Dkt. No. 62-2, McGoff Decl. ¶¶ 9–11.) The report indicated that a Google employee did not manually review the images after Google's proprietary hashing technology tagged the images as apparent child pornography.[5] (*Id.*)

5. NCMEC Forwarded the CyberTipline Report to the San Diego Internet Crimes Against Children ("ICAC") Task Force Program.

On or about June 17, 2015, NCMEC forwarded the CyberTipline Report to the San Diego ICAC Task Force Program. (Dkt. No. 62-3 at 17, Ex. 3.) NCMEC forwarded the information supplied by Google and the four image files to ICAC. (*Id.*) NCMEC did not forward the email itself. (*Id.*) NCMEC clarified, "Please be advised that NCMEC has

[5] As detailed above, *supra* Part B.2, Google's multi-tiered screening process ensured that at least one trained Google employee previously determined that duplicate copies of the four images constituted child pornography, added the four images to Google's repository of known child pornography images, and generated unique hash values for each offending image.

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." (*Id.*)

6. Homeland Security Investigation ("HSI") Special Agent ("SA") William Thompson Reviewed the CyberTipline Report, Visually Examined the Four Image Files, and Confirmed the Four Images Depict Child Pornography.

The San Diego ICAC office printed the report it received from NCMEC and the four attached image files. The printed report and images were given to SA Thompson. SA Thompson's review was limited to the contents of the CyberTipline Report and the four image files. He did not view or have access to Defendant's email at this time.

SA Thompson visually examined the four images and confirmed that they depict child pornography. Each of the images depicts a prepubescent minor engaged in a sex act, in line with Google's classification of the images as "A1" content. SA Thompson described the four images as follows.

1. 140005125216.jpg – This image depicts a young nude girl, approximately five (5) to nine (9) years of age, who is lying on her stomach with her face in the nude genital region of an older female who is seated with her legs spread. A second young girl, approximately five (5) to nine (9) years of age, is also visible in this image and she is partially nude with her vagina exposed. Google identified this image was uploaded on June 4, 2015, at 16:11:04 UTC.

2. 140005183260.jpg – This image depicts a young nude girl, approximately five (5) to nine (9) years of age, who is lying on top of an older nude female, approximately eighteen years of age. Within this image the girl's genital regions are pressed against one another and the older girl appears to be touching the face of the younger child with her tongue. Google identified this image was uploaded on June 4, 2015, at 16:11:21 UTC.

3. 140005129034.jpg – This image depicts a partially nude young girl, approximately five (5) to nine (9) years of age, 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. Google identified this image was uploaded on June 4, 2015, at 16:11:06 UTC.

4. 1400052000787.jpg – This image depicts a wider angle view of the previously referenced images possessing file names 140005125216.jpg and 140005129034.jpg as reported by Google.

(Dkt. No. 62-4, Ex. 4.)

7. SA Thompson Submitted Department of Homeland Security ("DHS") Summonses to Google and AT&T Internet Services Requesting Subscriber Information for soulrebelsd@gmail.com and jameskindle2012@gmail.com.

On July 6, 2015, SA Thompson submitted a DHS Summons to Google requesting subscriber information for email accounts soulrebelsd@gmail.com and jameskindle2012@gmail.com. (Dkt. No. 62 at 8; Dkt. No. 62-5 at 9–10.) Google provided the following information in response:

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

(*Id.*)

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. (*Id.*) AT&T Internet Services provided the following information in response:

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

(*Id.*)

On July 20, 2015, SA Thompson conducted database and law enforcement queries related to Defendant and obtained his name, date of birth, California driver's license number, registered vehicle (year, make, license number), and residential address. (*Id.*)

8. SA Thompson Obtained a State Search Warrant for the Email Account soulrebelsd@gmail.com.

On July 29, 2015, SA Thompson obtained a state search warrant for Defendant's Google email account soulrebelsd@gmail.com. (Dkt. No. 62-4, Ex. 4.) The July 29, 2015 state search warrant was the first warrant SA Thompson obtained in relation to the investigation. SA Thompson consulted with a Deputy District Attorney prior to presenting the affidavit to the judge for review. (*Id.* at 9.) Probable cause for the warrant was premised upon CyberTipline Report # 5074778, SA Thompson's review and description of the four images (as described above, *supra* Part A.6), and the subscriber information provided by Google and AT&T Internet Services. (*Id.* at 5–6.) SA Thompson's affidavit did not contain any mention of hash values, any description of Google's screening process for child pornography, or the A1 classification Google assigned to the four images. (*See generally* Dkt. No. 62-4, Ex. 4.)

After reviewing search warrant results, SA Thompson located dominion and control emails linking Defendant to the account. (Dkt. No. 62 at 9.) SA Thompson also discovered email exchanges between Defendant, using soulrebelsd@gmail.com, and Jenalyn Arriola, using jenalynarriolax3@gmail.com. (*Id.* at 9–10.) In these email exchanges, Defendant solicited the creation of child pornographiy for pay, and Arriola sent Defendant child pornography images and video files. (*Id.*)

9. SA Thompson Obtained a Search Warrant for Defendant's Residence.

On August 17, 2015, law enforcement obtained a state search warrant for Defendant's residence. (Dkt. No. 62-5, Ex. 5.) Probable cause for the warrant was based upon CyberTipline Report # 5074778, SA Thompson's review and description of the four images (as described above, *supra* Part A.6), subscriber information provided by Google and AT&T Internet Services, database and law enforcement queries, and physical

surveillance conducted at Defendant's residence. (*Id.* at 8–10.) SA Thompson consulted with a Deputy District Attorney prior to presenting the affidavit to the judge for review. (*Id.* at 13.)

The warrant was executed the next day on August 18, 2015. (Dkt. No. 62 at 11.) Defendant was located in the residence upon law enforcement's entry into the apartment. (*Id.*) Law enforcement seized multiple electronic devices from Defendant's residence. (*Id.*) During execution of the warrant, a San Diego Police Department ("SDPD") officer who was positioned on perimeter security notified investigators that he observed a backpack being tossed over Defendant's third floor balcony at the same time he heard the knock and notice upon Defendant's residence door. (*Id.*) SA Thompson searched the backpack and discovered Defendant's checkbook and a thumb drive. (*Id.*) During an on-scene forensic preview of the 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. (*Id.*)

10. Law Enforcement Conducted a Follow-Up Investigation of Jenalyn Arriola.

After obtaining subscriber information related to the Google account for jenalynarriolax3@gmail.com, law enforcement located Arriola. (Dkt. No. 62 at 12.) On August 20, 2015, SA Thompson advised Arriola of her *Miranda* rights, which she waived. (*Id.*) Arriola made a statement admitting to molesting two minor females and to producing child pornography depicting these molestations. (*Id.*) Arriola stated that she sent child pornographic images and videos to Defendant via text message and email. (*Id.*)

On August 31, 2015, SA Thompson obtained a search warrant for various Google accounts belonging to Arriola, including jenalynarriolax3@gmail.com. (Dkt. No. 62-6, Ex. 6.) SA Thompson stated in his affidavit that he had previously obtained a warrant for Defendant's email account. (*Id.* at 5.) SA Thompson consulted with a Deputy District

Attorney prior to presenting the affidavit to the judge for review. (*Id.* at 9.) Probable cause for the warrant was based upon information obtained from the results of the warrant executed on Defendant's email account as well as Arriola's statement. (*Id.* at 5–6.)

On September 8, 2015, Google responded to the search warrant and produced from the jenalynarriolax3@gmail.com 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. (*Id.*)

B. Procedural History

On October 15, 2015, Defendant 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). (Dkt. No. 1.) 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 Images of Minors Engaged in Sexually Explicit Conduct in violation of 18 U.S.C. § 2252(a)(2), and Possession of Matters Containing Images of Minors Engaged in Sexually Explicit Conduct in violation of 18 U.S.C. § 2252(a)(4)(B). (Dkt. No. 17.) The indictment also includes a criminal forfeiture allegation under 18 U.S.C. § 2253(a)–(b). (*Id.*) On November 12, 2015, Defendant was arraigned on the indictment and pleaded not guilty to the charges. (Dkt. No. 18.)

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. (Dkt. Nos. 32, 34.) On June 30, 2016, this Court accepted the guilty plea. (Dkt. No. 36.)

On February 3, 2017, Defendant filed a Motion to Withdraw his Guilty Plea. (Dkt. Nos. 44.) On April 14, 2017, the Court granted Defendant's motion, and Defendant's plea was withdrawn. (Dkt. No. 55.)

On April 28, 2017, Defendant filed the instant Motion to Suppress Evidence as a Result of an Illegal Search. (Dkt. No. 57.) Defendant moves to suppress the four image files tagged by Google's proprietary hashing technology, all evidence subsequently seized from Defendant's email account and residence, and all evidence seized from Arriola's email account and statements. (*Id.* at 14.) The Government opposed the motion on May 11, 2017. (Dkt. No. 62.) Defendant replied on May 15, 2017. (Dkt. No. 65.) On May 18, 2017, the Court conducted an evidentiary hearing and took the matter under submission. (Dkt. No. 67.)

DISCUSSION

Does a government agent's visual examination of a child pornography image that was digitally matched by an ISP's proprietary hashing technology to a duplicate image in the ISP's repository of confirmed child pornography images constitute a significant expansion of the ISP's earlier private search? It does not. While SA Thompson's visual inspection of four child pornography images flagged by Google's proprietary hashing technology expanded upon Google's private search, it was not a significant expansion. No search occurred for purposes of the Fourth Amendment. Defendant's motion to suppress is **DENIED** for the reasons set forth below.

I. Defendant Lacked a Reasonable Expectation of Privacy in the Four Child Pornography Files He Uploaded to His Google Email Account.

The contents of Defendant's email messages are protected by the Fourth Amendment. The Supreme Court has long held that the government cannot engage in a warrantless search of the contents of sealed mail. *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008) (citing cases). Analogizing email to physical mail, the Ninth Circuit concluded that the privacy interests in email and physical mail are identical. *Id.* Accordingly, while external information, such as the to/from addresses of e-mail messages, does not fall within the protective sweep of the Fourth Amendment, the contents of email messages may deserve Fourth Amendment protection. *Id.* at 510–11.

However, Defendant lacked an objectively reasonable expectation of privacy in the four child pornography files he uploaded to his Google email account. While Defendant held a subjective expectation of privacy in his Google email account at all relevant times, (*see* Dkt. No. 57-2, Declaration of Luke Noel Wilson ("Wilson Decl.") ¶¶ 3–5), Defendant's subjective expectation of privacy in the four child pornography attachments was not objectively reasonable or justifiable under the circumstances, *see Smith v. Maryland*, 442 U.S. 735, 740 (1979) (requiring an individual's subjective expectation of privacy to be objectively reasonable).

Specifically, Defendant agreed to Google's November 11, 2013 Terms of Service when he created his Google email account on March 13, 2014, and agreed to Google's April 14, 2014 Terms of Service by continuing to use his account. The April 14, 2014 Terms of Service alerted users that Google may "investigat[e] suspected misconduct," "review content to determine whether it is illegal or violates [Google's] policies," and "remove or refuse to display content that [Google] reasonably believe[s] violates [Google's] policies or the law."[6] (Dkt. No. 62-2 at 5, McGoff Decl. Ex. A.) This express monitoring policy regarding illegal content, which Defendant agreed to, rendered Defendant's subjective expectation of privacy in the four uploaded child pornography attachments objectively unreasonable. *C.f. United States v. Heckenkamp*, 482 F.3d 1142, 1147 (9th Cir. 2007) ("[P]rivacy expectations may be reduced if the user is advised that information transmitted through the network is not confidential and that the systems administrators may monitor communications transmitted by the user." (citing *United States v. Angevine*, 281 F.3d 1130, 1134 (10th Cir. 2002); *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000)).

[6] Google included the following caveat regarding its review of non-Google content: "But that does not necessarily mean that we review content, so please don't assume that we do." (*Id.*) However, this caveat does not negate Google's explicit statements alerting users that it may review user accounts for illegal content. Defendant's subjective belief that the illegal contents of his emails were entirely private is objectively unreasonable in light of Google's retention of the right to review his content for illegality.

In any event, the Court's resolution of the instant motion to suppress does not depend upon the finding that Defendant lacked an expectation of privacy in the four child pornography files he uploaded to his Google email account.[7] Rather, the Court's decision rests upon the conclusion that the government did not significantly expand upon Google's private search. *See infra* Part II.

II. A Search Did Not Occur Within Meaning of the Fourth Amendment.

"The Fourth Amendment's proscriptions on searches and seizures are inapplicable to private action." *United States v. Tosti*, 733 F.3d 816, 821 (9th Cir. 2013) (citing *United States v. Jacobsen*, 466 U.S. 109, 113–14 (1984)). "Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information." *Id.* (quoting *Jacobsen*, 466 U.S. at 117). Rather, the Fourth Amendment "is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated." *Id.* (quoting *Jacobsen*, 466 U.S. at 117). Accordingly, 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.* (quoting *Jacobsen*, 466 U.S. at 115).

Jacobsen is instructive. In *Jacobsen*, employees of Federal Express, a private freight carrier, were examining a damaged package pursuant to a company policy regarding insurance claims when they observed a white powdery substance concealed within eight layers of wrappings. 466 U.S. at 111. The employees opened the package, found a ten-inch tube within the box, cut open the tube, and saw a series of four layers of zip-lock plastic bags, the innermost of which contained white powder. *Id.* The employees subsequently notified the Drug Enforcement Administration ("DEA"), placed the bags back into the tube, and then returned the tube back into the box. *Id.* The first

[7] To be clear, the Court does not reach the question of whether Defendant's expectation of privacy in the contents of his Google email account was extinguished across the board by his agreement to Google's Terms of Service. SA Thompson never viewed the contents of Defendant's email without a warrant—he viewed only the four child pornography photographs Defendant uploaded.

DEA agent to arrive saw that the tube had been slit open. *Id.* He first removed the four plastic bags from the tube and saw the white powder. *Id.* He next opened the four bags, removed a trace of the white substance with a knife blade, and performed a field test on the substance. *Id.* at 111–12. The field test identified the powder as cocaine. *Id.* at 112. Subsequently, other DEA agents arrived, conducted a second field test, rewrapped the package, and obtained a warrant to search the location to which the package was addressed. *Id.*

The Supreme Court concluded that the wrapped parcel was an "effect" within meaning of the Fourth Amendment, given that "[l]etters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy." *Id.* at 114. The Supreme Court divided the invasions of privacy of the wrapped parcel into three steps. First, the Supreme Court observed that "[t]he initial invasions of [the] package were occasioned by private action. Those invasions revealed that the package contained only one significant item, a suspicious looking tape tube. Cutting the end of the tube and extracting its contents revealed a suspicious looking plastic bag of white powder." *Id.* at 115. These invasions "did not violate the Fourth Amendment because of their private character." *Id.*

Next, the Supreme Court broke down the DEA agents' invasions of privacy into two steps: "first, they removed the tube from the box, the plastic bags from the tube and a trace of powder from the innermost bag; second, they made a chemical test of the powder." *Id.* at 118. The first set of government actions did not violate the Fourth Amendment. "The agent's viewing of what a private party had freely made available for his inspection did not violate the Fourth Amendment," even if the white powder was not initially in plain view, because there was a "virtual certainty that nothing else of significance was in the package" and that the agent could "learn nothing that had not previously been learned during the private search." *Id.* at 118–19. After the private search, "the package could no longer support any expectation of privacy." *Id.* at 121.

Nor was the agent's warrantless seizure of the package and its contents unreasonable under the Fourth Amendment. *Id.* at 119–20.

> [S]ince it was apparent that the tube and plastic bags contained contraband and little else, this warrantless seizure was reasonable, for it is well-settled that it is constitutionally reasonable for law enforcement officials to seize "effects" that cannot support a justifiable expectation of privacy without a warrant, based on probable cause to believe they contain contraband.

Id. at 121–22.

The second set of government actions also did not violate the Fourth Amendment. "The field test at issue could disclose only one fact previously unknown to the agent—whether or not a suspicious white powder was cocaine." *Id.* at 122. Such a test "does not compromise any legitimate interest in privacy." *Id.* at 123. The Supreme Court clarified that its conclusion did not depend on the result of the test. *Id.*

> 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. But even if the results are negative—merely disclosing that the substance is something other than cocaine—such a result reveals nothing of special interest. Congress has decided . . . to treat the interest in "privately" possessing cocaine as illegitimate; thus governmental conduct that can reveal whether a substance is cocaine, and no other arguably "private" fact, compromises no legitimate privacy interest.

Id.

Following *Jacobsen*, the Ninth Circuit concluded in *Tosti* that no search had occurred within the meaning of the Fourth Amendment, where the government detectives' searches of child pornography on the defendant's computer derived from a private party's original search. *See* 733 F.3d at 821. In *Tosti*, the defendant took his computer to a CompUSA store for service. *Id.* at 818. A CompUSA employee was servicing the defendant's computer when he discovered and opened various folders and subfolders containing many child pornography images. *Id.* at 818–19. The employee contacted the police, and two detectives responded to the call and arrived at the store. *Id.* at 819. Upon discerning that thumbnails of pictures on the screen depicted child

pornography, the first detective instructed the CompUSA employee to open the images in a slideshow format so that he could view the enlarged images one by one. *Id.* The second detective scrolled through the thumbnail images on the screen and observed that the images depicted child pornography. *Id.* The detectives then seized the defendant's computer, and a search warrant for the defendant's computer, residence, office, and two vehicles was subsequently obtained based on the detectives' observations. *Id.*

The Ninth Circuit upheld the district court's denial of the defendant's motion to suppress the fruits of the detectives' warrantless search of his computer. *Id.* at 821. To start, the defendant had "voluntarily tak[en] his computer to CompUSA for repairs [and] 'understood that a technician at CompUSA would have temporary custody of the computer, and would inspect it as needed to complete the requested repairs.'" *Id.* The detectives' warrantless viewing of the photographs did not trigger the Fourth Amendment because the CompUSA employee's "prior viewing of the images had extinguished [the defendant's] reasonable expectation of privacy in them." *Id.* The detectives had viewed only the photographs that the private employee had already viewed. *Id.* at 822. The detectives' viewing of enlarged versions of the thumbnails was not a significant expansion of the private party's search, as "the police learned nothing new through their actions." *Id.*

Applying *Jacobsen* and *Tosti* to the facts at hand, the Court concludes that Google conducted a private search of the contents of Defendant's email, and that the government's expansion of Google's private search was not significant.

A. Google Conducted an Extensive Private Search of Defendant's Email.

As detailed in the Court's factual findings, Google voluntarily undertakes a multi-tiered process to screen user content for child pornography. A team of Google employees receives training from counsel on the federal statutory definition of child pornography and how to recognize child pornography on Google's products and services. After at least one trained employee has viewed an image and determined that it is apparent child pornography, the offending image is assigned a unique hash value and added to Google's

repository of hashes of apparent child pornography. Google's product abuse screening system then searches its products and services for hash values that match hash values already catalogued in its repository of known child pornography images. As a result of this extensive screening process, all images tagged by Google's proprietary hashing technology—including the four uploaded files Google discovered in Defendant's email—are duplicate images of confirmed child pornography images that have already been viewed and previously identified by trained Google employees.

Google's extensive screening process constituted a private search of Defendant's email account. This conclusion is in line with Judge Kozinski's observations about hashing technology in *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010) (Kozinski, J., concurring). Judge Kozinski acknowledged that "the government has sophisticated hashing tools at its disposal that allow the identification of well-known illegal files (such as child pornography) without actually opening the files themselves," and offered the admonition that "[t]hese and similar search tools should not be used without specific authorization in the warrant, and such permission should only be given if there is probable cause to believe that such files can be found on the electronic medium to be seized." 621 F.3d at 1179. If the government may not use such sophisticated hashing tools and similar search technology without specific authorization in a warrant, the use of hashing technology to identify illegal files like child pornography certainly constitutes a search. Here, by extension, Google's use of its proprietary hashing technology to screen Defendant's email account constituted a private search.

B. SA Thompson's Warrantless Viewing of the Four Child Pornography Images Was Not a Significant Expansion of Google's Private Search.

SA Thompson's viewing of the four child pornography attachments arguably expanded upon Google's private search. At least one Google employee had previously viewed each of the four child pornography images Defendant uploaded to his account; however, an employee did not open the four file attachments after Google's hashing technology tagged the four images as child pornography. Nevertheless, even assuming

arguendo that SA Thompson's viewing of the four images was an expansion of Google's private search, it was not a significant expansion.

The facts of this case are even stronger than those of *Jacobsen*. Here, Google's private search far exceeded the Federal Express employees' private search of the damaged parcel in *Jacobsen*. Whereas the Federal Express employees merely suspected that the white powder in the damaged parcel was contraband, Google had previously confirmed that each of the four images in Defendant's email was child pornography. SA Thompson already knew, before visually examining the images, from the "A1" classification that each of the four images depicted a prepubescent minor engaged in a sex act. (*See* Dkt. No. 62-3 at 14, Ex. 3.) Compared to *Jacobsen*, there was even more of a "virtual certainty" that SA Thompson could "learn nothing that had not previously been learned during the private search." *Jacobsen*, 466 U.S. at 118–19.

Moreover, not only did Google search Defendant's email, Google extracted the four child pornography images from the email. Unlike the DEA agents in *Jacobsen*, who removed the tube from the box, removed the innermost plastic bags from its enclosing layers, and removed a trace amount of cocaine powder from the innermost bag for testing, SA Thompson did not perform any analogous actions. Rather, because Google performed the removal functions on the front end, SA Thompson already had access to (and indeed, only had access to) the four illegal files Google extracted from Defendant's email. Accordingly, like the detectives in *Tosti* who viewed images a private employee had determined to be child pornography, SA Thompson's viewing of the four images allowed SA Thompson to "learn[] nothing new." *Tosti*, 733 F.3d at 822. SA Thompson's expansion of Google's private search "d[id] not expose noncontraband items that otherwise would remain hidden from public view."[8] *Jacobsen*, 466 U.S. at 124

[8] Citing *United States v. Jones*, 565 U.S. 400 (2012), Defendant argues cursorily that SA Thompson "committed a trespass of Mr. Wilson's house and effects when it illegally searched and [sic] seized his email." (Dkt. No. 65 at 6.) Given the Court's conclusion that the government agent's search did not significantly expand upon Google's private search, and that a search did not occur within meaning of the

(quoting *United States v. Place*, 462 U.S. 696, 707 (1983)); *see also Walter v. United States*, 447 U.S. 649, 657 (1980) (concluding that the government's actual viewing of films implicated the Fourth Amendment because it significantly expanded upon the private party's prior search, which had involved only a visual inspection of the labels on the outside of the film boxes).

Defendant cites *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), *reh'g denied* (Oct. 4, 2016), in support of his argument that the Government unconstitutionally expanded upon Google's private search. (Dkt. No. 65 at 2–3.) However, in *Ackerman*, the state actor not only viewed the child pornography file that was the subject of AOL's private hash search, but opened the email itself and viewed three other non-child pornography attachments. *Ackerman*, 831 F.3d at 1306–07. There, these actions expanded upon AOL's private search and "risk[ed] exposing private, noncontraband information that AOL had not previously examined." *Id.* at 1307. Here, SA Thompson viewed only the four child pornography files that were the target of Google's private search, and nothing more. As such, "'the governmental conduct could [have] reveal[ed] nothing about noncontraband items.'" *Id.* at 1306 (quoting *Jacobsen*, 466 U.S. at 124 n.24)).

III. The Government's Alternative Arguments Do Not Succeed.

Although the Government's remaining arguments do not affect disposition of the instant motion, the Court nonetheless addresses the Government's alternative arguments for instructive purposes.

/ / / /

Fourth Amendment, the question of whether or not *Jones* applies does not affect the Court's disposition. To the extent *Jones* creates any tension with *Jacobsen* and its progeny, *Jones* did not expressly overrule or limit *Jacobsen*. The DEA agents' *de minimis* "trespass" upon the defendant's property—their destruction of the defendant's possessory interests in a trace amount of cocaine powder—did not render the agents' warrantless search and seizure constitutionally infirm. *See Jacobsen*, 466 U.S. at 126 ("To the extent that a protected possessory interest was infringed, the infringement was *de minimis* and constitutionally reasonable.").

A. Excision of the Tainted Evidence in the Affidavit Would Not Support Issuance of the Search Warrant for Defendant's Email Account.

"The mere inclusion of tainted evidence in an affidavit does not, by itself, taint the warrant or the evidence seized pursuant to the warrant. A reviewing court should excise the tainted evidence and determine whether the remaining, untainted evidence would provide a neutral magistrate with probable cause to issue a warrant." *United States v. Vasey*, 834 F.2d 782, 788 (9th Cir. 1987) (citing *United States v. Driver*, 776 F.2d 807 (9th Cir. 1985)).

Here, excising the tainted evidence from the affidavit would not support issuance of the search warrant for Defendant's email account. (*See* Dkt. No. 62-4, Ex. 4.) Probable cause for the warrant was premised upon CyberTipline Report # 5074778, SA Thompson's review and description of the four images, and the subscriber information provided by Google and AT&T Internet Services. (*Id.* at 5–6.) SA Thompson's affidavit did not contain any mention of hash values, any description of Google's screening process for child pornography, or the A1 classification Google assigned to the four images. (*See generally* Dkt. No. 62-4, Ex. 4.) Had the affidavit included information about Google's screening process for child pornography, there may have been sufficient information in the affidavit to establish probable cause, even after excision of the tainted evidence. However, after removing SA Thompson's description of the four images from the affidavit, the only remaining salient information states that "Google became aware of four (4) image files depicting suspected child pornography which were uploaded to an email on June 4, 2015." (*Id.* at 5.) This bare statement, standing alone, would be insufficient to establish probable cause for issuance of a search warrant for Defendant's entire email account.[9]

[9] The Government also briefly argues the exclusionary rule would not apply to evidence subsequently obtained from Arriola and from the backpack Defendant threw out of his apartment during law enforcement's search of his residence. (Dkt. No. 62 at 18.) The Government takes an unduly narrow view of the evidence and has not meaningfully argued how these sources of evidence were not fruits of

B. The Good Faith Exception Would Not Apply.

The good faith exception to the exclusionary rule originated in *United States v. Leon*, 468 U.S. 897 (1984). In *Leon*, the Supreme Court "held that the Fourth Amendment exclusionary rule should not be applied so as to bar the use in the prosecutor's case-in-chief of evidence obtained by officers acting in reasonable reliance on a search warrant issued by a detached and neutral magistrate but ultimately found to be invalid." *United States v. Vasey*, 834 F.2d at 789 (citing *Leon*, 468 U.S. at 900, 926).

In *Vasey*, the Ninth Circuit rejected the government's argument that the good faith exception applied, where the officer "conducted an illegal warrantless search and presented tainted evidence obtained in this search to a magistrate in an effort to obtain a search warrant." *Id.* There, "[t]he search warrant was issued, at least in part, on the basis of this tainted evidence. The constitutional error was made by the officer in this case, not by the magistrate as in *Leon*." *Id.* Observing the Supreme Court's admonition that "the exclusionary rule should apply (i.e. the good faith exception should not apply) if the exclusion of evidence would alter the behavior of individual law enforcement officers or the policies of their department," the Ninth Circuit concluded that the officer's "conducting an illegal warrantless search and including evidence found in this search in an affidavit in support of a warrant is an activity that the exclusionary rule was meant to deter." *Id.*

Here, if SA Thompson's warrantless viewing of the four images constituted an illegal search, the good faith exception would not apply to prevent operation of the

SA Thompson's initial warrantless search. While it is true that Arriola admitted to law enforcement that she had sent and received communications about and containing child pornography to and from Defendant, the evidence shows that the Government discovered Arriola only after executing a search of Defendant's Google email account. And while Defendant's abandonment of his backpack suggests that he had relinquished a reasonable expectation of privacy in his property, the evidence indicates that he did so only upon law enforcement's execution of the search warrant for Defendant's residence. Probable cause for the search warrant for Defendant's residence depended upon results of the search warrant for Defendant's email account, which in turn depended upon SA Thompson's visual examination of the four images.

exclusionary rule. Unlike in *Leon*, Defendant alleges that SA Thompson made the constitutional error in this case. The magistrate's issuance of the warrant and consideration of the evidence would not "sanitize the taint of the illegal warrantless search." *Id.* An illegal warrantless search would be precisely the sort of conduct the exclusionary rule was meant to deter. *See id.*; *see also United States v. Camou*, 773 F.3d 932, 945 (9th Cir. 2014) ("The Supreme Court has never applied the good faith exception to excuse an officer who was negligent himself, and whose negligence directly led to the violation of the defendant's constitutional rights.").

In sum, if SA Thompson's warrantless viewing of the four images constituted an illegal search, neither excising the tainted evidence from the affidavit nor the good faith exception would prevent operation of the exclusionary rule. Nevertheless, as detailed above, *supra* Part II.B, SA Thompson's visual examination of the four images did not significantly expand upon Google's private search, and thus did not constitute a search within meaning of the Fourth Amendment.

CONCLUSION

For the foregoing reasons, the Court **DENIES** Defendant's motion to suppress. (Dkt. No. 57.)

IT IS SO ORDERED.

Dated: June 26, 2017

Hon. Gonzalo P. Curiel
United States District Judge