IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

UNITED STATES OF AMERICA, **Plaintiff,** **v.** **MICHAEL L. STRATTON,** **Defendant.**	**Case No. 15-40084-01-DDC**

MEMORANDUM AND ORDER

This matter comes before the court on defendant Michael L. Stratton's Motion to Suppress Evidence (Doc. 19). Defendant asserts that his Fourth Amendment rights were violated when Sony searched information stored on his PlayStation3 gaming device and, as a result, that the court must suppress (1) evidence the National Center for Missing and Exploited Children ("NCMEC") obtained from searching his electronic communications; (2) evidence law enforcement officers obtained from searching defendant's residence; and, (3) statements defendant made to law enforcement during the search. For reasons explained below, the court denies defendant's Motion.

I. Background

The court finds the following facts from evidence presented at the June 20, 2016 and November 10, 2016 motion hearings and, where undisputed, the parties' briefs.

Sony Computer Entertainment America, LLC ("Sony"), as a "professional entity," is governed by 18 U.S.C. § 2258. This provision states: "A person who, while engaged in a professional capacity . . . learns of facts that give reason to suspect that a child has suffered an incident of child abuse . . . and fails to make a timely report . . . shall be fined under this title or

imprisoned not more than 1 year or both." Sony's network—the PlayStation Network ("PSN")—is an online gaming network. The Sony PlayStation3 ("PS3") is Sony's online gaming device. The PS3 accesses the PSN. Then, the PS3 allows PSN account holders to communicate with other users online. These communications are like email communications. Users can send each other messages and attachments. And if, while monitoring these messages and attachments, Sony learns of facts that give reasons to suspect child abuse, § 2258 requires Sony to report its suspicions to law enforcement.

To access the PSN, a user must have a PSN account. And to sign up for a PSN account, a user must agree to PSN's terms of service. In December 2008, the PSN terms of service required a person signing up for a PSN account to agree to the following:

> You may not take any action, or upload, post, stream, or otherwise transmit any content . . . that [Sony], in its sole discretion, finds offensive, hateful, or vulgar. This includes but is not limited to, any content or communication that [Sony] in its sole discretion deems racially, ethnically, religiously, or sexually offensive. . . . You may not upload, post, stream, access, or otherwise transmit any content that you know or should have known to be infringing, or that violates, any third party rights, any law . . .
>
> You may not conduct any activities that violate any local, state or federal laws . . .
>
> there is no requirement or expectation that [Sony] will monitor or record any online activity on PSN, including communications. However [Sony] reserves the right to monitor and record any online activity and communication throughout PSN and you give [Sony] your express consent to monitor and record your activities . . . Any data collected in this way, including the content of your communications, the time and location of your activities, your Online ID and IP address and other related information may be used by us to enforce this Agreement or protect the interests of [Sony], its users, or licensors. Such information may be disclosed to the appropriate authorities or agencies.

Thomas Meininger, an operations supervisor in Sony's Customer Service Department, testified about the terms of service agreement at the hearing on November 10, 2016. He testified that the PSN is an online gaming community. So, Sony has an interest in making the PSN a safe

place for people to play online. According to Mr. Meininger, Sony thus has an interest in monitoring its users' activity.

Sony monitors misuses of the PSN through PSN user reports. These are called "grief reports." When the PSN user comes across content they wish to report, the user hits the "Cross-Media Bar" button. This button brings up a "reporting option." The reporting option asks the user to describe the reason for the grief report. PSN users use these grief reports to report things like offensive messages, offensive attachments to messages, or offensive user IDs. When the PSN user submits the grief report, it goes to Sony's Moderation Department.

Once the Moderation Department receives a report, a Moderator opens the report and reviews its content. The Moderator then determines whether the content violates Sony's Terms of Service Agreement. If the Moderator determines that the content contains a minor offense under the agreement (such as verbal abuse or some other minor form of harassment), the Moderator clicks a button to put the report in a queue. Once in this queue, another member of the Moderation Team takes action on the report. According to Mr. Meininger, a minor offense warrants a minor response from the Moderation Team. Typically, this is something like a warning message that the user has violated PSN's Terms of Service Agreement. More serious offenses warrant suspending the PSN account for several days. And, if the offense seems potentially illegal or life-threatening, the Moderator forwards the report to the Security Team. The Moderator does this by hitting a "Single Point of Contact" ("SPOC") button. Once the Moderator hits the SPOC button, the report moves to another queue for the Security Team to evaluate. The Moderator can no longer access it.

Once a report is "SPOCed" to the Security Team, a member of that team reviews the report and decides what to do next. Mr. Meininger testified that he was not sure whether any law

enforcement officer was involved in Sony's day-to-day operations. Mr. Meininger testified, however, that law enforcement gets involved if the Security Team determines that Sony should report the customer grief report to authorities.

On June 6, 2012, Sony received a customer grief report about PSN user "Susan_14." The grief report alerted Sony to a message and an attached image sent from Susan_14's account. Apparently, this report eventually was "SPOCed" because it was sent to Sony's Security Team.

On August 8, 2012, Sony's Security Manager, Mariko Kawaguchi, reported Susan_14 to NCMEC to comply with § 2258. Ms. Kawaguchi's NCMEC report included Susan_14's user profile information—email address, home address, and the date when the user opened the PSN account. The report also included Susan_14's IP address, a screenshot of the reported message, and a screenshot of the attached image. NCMEC concluded that the image did not contain child pornography and filed a report concluding as much.

On December 19, 2012, Ms. Kawaguchi submitted a second "revived" report to NCMEC. This revived report bore the same case number as the August 8, 2012 report. This revived report was labeled "case update" and included several additional files that Sony had downloaded from Susan_14's account. In her affidavit, Ms. Kawaguchi stated that Sony typically revives reports to NCMEC for one of three reasons: (1) a user has filed an additional grief report about the account; (2) the account has violated "community standards"; or, (3) at law enforcement's request. In this revived report, Sony informed NCMEC that Susan_14[1] had uploaded several more files warranting NCMEC's review. On January 8, 2013, NCMEC confirmed that the downloaded images included child pornography.

[1] The parties' briefs do not explain why some of the grief reports discussed in their briefs complain about "Susan_14" and others "Susan_Nude" or "Susan_nude." The court concludes that this disparity is not material and these usernames all refer to the same PSN user account. For consistency, this Order uses the username "Susan_14."

About eight months later, on July 25, 2013, Sony received two more grief reports about Susan_14. After reviewing both reports, Sony sent another report to NCMEC on July 30, 2013. According to the report, Susan_14 had sent messages to other PSN users with text including "u want to see naked kids tonight" and "Friend Request. Do you have child porn." Sony also reported to NCMEC that it had downloaded more images from Susan_14's account and found photos of nude children. The children ranged in age from 6 to 12, and the photographs showed them posing in sexually suggestive ways. Sony also sent these images with the July 2013 report.

NCMEC determined that the files contained child pornography and made the files available to law enforcement for independent review. Authorities served a subpoena on Google for account information for the username "nudesusan14@gmail.com." Google's response included an IP history log. Authorities served a subsequent subpoena on CenturyLink to identify the user of the IP address, which returned an IP address for defendant's residence in Burlington, Kansas.

The FBI has a liaison who works at the NCMEC office. This liaison sent information about Susan_14's PS3 account, the subpoenas, and defendant's home address to Senior Special Agent Angie Jones. Agent Jones works for the Kansas Bureau of Investigation and is assigned to the FBI child exploitation task force. As the investigation's lead agent, Agent Jones reviewed the information that Sony had provided to NCMEC, the subpoenas issued to Google and CenturyLink, their responses, and other publically available information. On November 1, 2013, Agent Jones secured a warrant to search defendant's residence in Burlington. The affidavit supporting the search warrant contained the following information: (1) the two customer grief reports Sony received on July 25, 2013; (2) the PSN user profile for Susan_14; (3) Sony's past reports of account suspensions for Susan_14; (4) the photo downloads Sony had retrieved from

Susan_14's account; (5) 10 archives Sony had downloaded from Susan_14's account (they included images of partially undressed children); (6) results from the administrative subpoena served on Gmail seeking the email address: nudesusan14@gmail.com; and, (7) results from the administrative subpoena served on CenturyLink for the IP address 76.7.2.212.142 connected to nudesusan14@gmail.com, which linked this IP address to a Burlington, Kansas address. Based on these submissions, United States Magistrate Judge Gary Sebelius issued a search warrant.

Officers executed the search warrant at defendant's home on November 1, 2013. They discovered images of suspected child pornography on defendant's PS3. During the search, authorities confronted defendant. Defendant ultimately told the officers that he owned the PS3 and used it to obtain images of nude children.

Defendant's Exhibit 102 is an archived document that logs a June 27, 2012 meeting between someone at Sony and the FBI. The information reads: "6/27/12 Meeting with FBI to discuss case and hand over data. Filed with NCMEC 8/8/12. 12/19/12: Case re-filed with additional information." At the hearing on November 10, 2016, Agent Jones testified that she did not know anything about this meeting other than what she had learned about it from defense counsel at the hearing. Agent Jones also testified that during the hearing she asked her colleagues to search the FBI database for any information about "Susan_14," "Mariko Kawaguchi," or "June 27, 2012." Their searches did not turn up any information in the database. Agent Jones testified that she remembers seeing two emails from someone at Sony while she was working on the case. After the November 10, 2016 hearing, defendant tried to compel production of any correspondence between Sony and the FBI. *See* doc. 48 (defendant's motion to compel production of relevant emails and subpoenas); doc. 52 (order granting defendant's Motion to Compel). The FBI did not produce any responsive documents.

II. Legal Standard

The Fourth Amendment to our Constitution protects persons against unreasonable searches and seizures in their "persons, houses, papers, and effects." U.S. Const. amend. IV. "The basic purpose of this Amendment . . . is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Camara v. Mun. Court of City & Cnty. of S.F.*, 387 U.S. 523, 528 (1967). "The exclusionary rule has traditionally barred from trial physical, tangible materials obtained either during or as a direct result of an unlawful" search or seizure. *Wong Sun v. United States*, 371 U.S. 471, 485 (1963).

III. Analysis

At the outset, the parties dispute whether the Fourth Amendment applies to the search at issue here. Neither party disputes that Susan_14's messages, attachments, and image downloads are "papers" and "effects" for Fourth Amendment purposes. But the government asserts that no Fourth Amendment search occurred because Sony instigated the initial search as a private entity. And, the government also asserts that, regardless of Sony's status, the Fourth Amendment does not protect the content located on defendant's PS3. Finally, the government contends that even if the Fourth Amendment applies, the court should deny defendant's Motion to suppress because the good faith exception to the exclusionary rule applies. The court addresses each argument, in turn, below.

A. Whether the Fourth Amendment Applies

1. Sony acted as a private entity when it searched defendant's PS3 content

Defendant concedes that Sony is not a government entity. But defendant asserts that Sony acted as a government agent when it searched images on Susan_14's account.

The Fourth Amendment 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 or with the participation or knowledge of any governmental official." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). To determine whether a private entity acted as a government agent when it conducted a search, the Tenth Circuit uses a two-part test: "1) whether the government knew of and acquiesced in the intrusive conduct, and 2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends." *United States v. Souza*, 223 F.3d 1197, 1201 (10th Cir. 2000).

Our Circuit has not addressed whether electronic service providers, like Sony, act as government agents when they monitor their users' activities on their servers. But, the Circuits that have addressed the question uniformly reject the government agent theorem. *See United States v. Cameron*, 699 F.3d 621, 638 (1st Cir. 2012) ("[I]f Yahoo! chose to implement a policy of searching for child pornography, it presumably did so for its own interests."); *United States v. Stevenson*, 727 F.3d 826, 831 (8th Cir. 2013) ("AOL's decision on its own initiative to ferret out child pornography does not convert the company into an agent or instrument of the government for Fourth Amendment purposes. . . . AOL's voluntary efforts to achieve a goal that it shares with law enforcement do not, by themselves, transform the company into a government agent."); *United States v. Richardson*, 607 F.3d 357, 366 (4th Cir. 2010) (holding that AOL's scanning of email communications for child pornography did not trigger the Fourth Amendment's warrant requirement because no law enforcement officer or agency asked the provider to search or scan the defendant's emails).

But defendant argues that Sony acted as a government agent under the standard the Tenth Circuit articulated in *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016). In *Ackerman*,

the Circuit considered whether NCMEC is a government entity, or alternatively, acts as a government agent when it creates and maintains CyberTipline reports for Congress. It held that NCMEC is a governmental entity, or at the very least, that NCMEC acts as a government agent when it maintains the CyberTipline, reviews emails and attachments sent to the CyberTipline, and reports illegal content to law enforcement. *Id.* at 1296–1304. According to *Ackerman*, "an agency relationship is usually said to 'result[ ] from the manifestation of consent by one person to another that the other shall act on his behalf and subject to his control, and consent by the other so to act.'" *Id.* at 1301 (quoting Restatement (Second) of Agency § 1). And *Acerkman* found that NCMEC's comprehensive statutory structure suggested that Congress both "knew of and acquiesced" to NCMEC's actions. *Id.* at 1301.

But, *Ackerman* discusses the comprehensive statutory structure governing *NCMEC*. *See id.* at 1301–02 (Congress statutorily required AOL to forward emails containing child pornography to NCMEC, statutorily required NCMEC to maintain the CyberTipline to receive these emails, statutorily permitted NCMEC to review these emails and attachments, and statutorily required NCMEC to report illegal behavior to law enforcement authorities); *see also* 42 U.S.C. § 5773(b) (the primary statute mandating NCMEC's collaboration with federal law enforcement). The only similar statute governing Sony is 18 U.S.C. § 2258. And § 2258 only requires Sony to file a report if it learns of facts that suggest an incident of child abuse. Unlike the statute governing NCMEC, § 2258 does not require Sony to act affirmatively to monitor its users' accounts, review its users' downloads, or maintain any sort of reporting system for abuse of Sony's PSN. Sony monitors its users' accounts to protect its own interests in a safe online gaming community. Nothing in § 2258, the parties' briefs, or in the evidence presented at the

June 20, 2016 and November 10, 2016 hearings suggests that Sony consented to act on behalf of the government or subject to its control.

Defendant contends that a meeting occurred on June 27, 2012, between someone at Sony and the FBI "to discuss [the] case and hand over data," and that this is evidence that Sony was working with the FBI "even before information was sent to NCMEC." Doc. 58 at 22. And, according to defendant, Sony worked with law enforcement's consent when Sony retrieved images downloaded onto Susan_14's account. Defendant contends that Sony did this to comply with § 2258, and thus Sony acted in furtherance of the government's purpose.

But, before the meeting on June 27, 2012, Sony already had received a customer grief report about Susan_14 on June 6, 2012. So, even before law enforcement allegedly became involved, Sony was alerted to a complaint about Susan_14. And, the court finds Sony acted to protect its own interests in a safe online gaming community when it reviewed the messages and attachments referenced in the June 6, 2012 grief report.

Defendant also contends that the case revival in December 2012 suggests "involvement and consent of law enforcement." *Id.* Defendant's argument rests on Ms. Kawaguchi's affidavit where she discusses "revived" cases. *Id.* at 37. According to Ms. Kawaguchi, "[i]f a child protection case sent to NCMEC was considered a 'revived' case, this meant that there was a record of a prior complaint at [Sony] for that individual or account." *Id.* And "[s]ubsequent complaints, additional escalated community standards violations or Grief Reports, any law enforcement request or additional inquiry from NCMEC would result in a case being revived." *Id.* Defendant contends that because no new grief reports about Susan_14 were filed between June 6, 2012, and December 19, 2012, the case must have been revived at the FBI or NCMEC's request.

But the court finds no evidence suggesting law enforcement requested Sony to revive the case. Nothing in the evidence suggests that Sony was acting to pursue anything other than its own interests when it revived the case and sent additional information to NCMEC. Sony's Terms of Service Agreement explicitly provided that users "may not take any action, or upload, post, stream, or otherwise transmit any content . . . that [Sony], in its sole discretion, finds offensive, hateful, or vulgar." Sony reserved the right to monitor and record online activity, and, according to Mr. Meininger, it did so to further its own interests in a safe online gaming community. And without any evidence that Sony acted at the government's request, the court cannot conclude that Sony acted as a government agent when it searched the images stored on defendant's PS3. The Fourth Amendment thus does not apply to Sony's search.

2. NCMEC did not exceed the scope of Sony's private search

Defendant asserts that even if the Fourth Amendment does not apply to Sony's search, NCMEC triggered Fourth Amendment protections when it exceeded the scope of Sony's private search. The "private search doctrine" is "often associated with" the holding in *United States v. Jacobsen*. *Ackerman*, 831 F.3d at 1305. In *Jacobsen*, the Supreme Court held that "[o]nce frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information." 466 U.S. at 117. It is now settled that even a "wrongful search . . . conducted by a private party does not violate the Fourth Amendment." *Walter v. United States*, 447 U.S. 649, 656 (1980). And, "such private wrongdoing does not deprive the government of the right to use evidence that it has acquired lawfully." *Id.*

But the private search doctrine is limited. The Supreme Court has analogized a private search to an authorized official search. *Id.* at 657. That is, "when an official search is properly

authorized—whether by consent or by the issuance of a valid warrant—the scope of the search is limited by the terms of its authorization." *Id.* And, if "a properly authorized official search is limited by the particular terms of its authorization, at least the same kind of strict limitation must be applied to any official use of a private party's invasion of another person's privacy." *Id.* In other words, if the results of the private search are turned over to the government, the government "may not exceed the scope of the private search" unless it has a right to conduct an independent search. *Id.*; *see also Jacobsen*, 466 U.S. at 122 ("The question remains whether the additional intrusion . . . exceeded the scope of the private search"). So, the question for the court is whether NCMEC exceeded the scope of Sony's private search and thus violated defendant's Fourth Amendment rights. This is the same issue the Tenth Circuit considered in *Ackerman*. And defendant asserts that *Ackerman* compels a finding of a Fourth Amendment violation here.

In *Ackerman*, the defendant sent an email containing child pornography. *Ackerman*, 831 F.3d at 1294. But, before the email reached its intended recipient, the defendant's Internet Service Provider ("ISP"), AOL, thwarted its transmission. *Id.* AOL apparently used an automated filter designed to stop its users from trasnmitting child pornography. *Id.* When one of these filters detected such an image in an email sent by an AOL user, AOL automatically stopped its delivery and reported the email to NCMEC. *Id.*

In its analysis, the Circuit first determined that NCMEC was a governmental entity. *Id.* at 1300. Then it considered whether NCMEC had violated the defendant's Fourth Amendment rights when it opened the email and attachments that AOL submitted to NCMEC. *Id.* at 1305. The Tenth Circuit concluded NCMEC had violated the defendant's Fourth Amendment rights. *Id.* at 1306–07.

But in *Ackerman*, no one from AOL ever actually opened the incriminating email or plaintiff's attached images before sending them to NCMEC. *Id.* at 1294. Instead, AOL's filter relied on "hash value matching." *Id.* "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." *Id.* AOL's filter worked "by identifying the hash values of images attached to emails sent through its mail servers." *Id.* The hash values then were compared to hash values of images AOL employees previously deemed as child pornography. *Id.* Emails containing images with a matching "hash value" were "automatically weeded out" and forwarded in a report to NCMEC's CyberTipline. *Id.* Then, a NCMEC analyst opened the email and viewed the attached images. *Id.*

In *Ackerman*, AOL's filter identified one of four images attached to the defendant's email as child pornography. *Id.* As soon as AOL identified the hash value match, it forwarded the email in a report submitted to NCMEC. *Id.* The NCMEC analyst viewed the email and the four image attachments and determined that all four of the attached images—not just the one that AOL's filter had identified—qualified as child pornography. *Id.* So, *Ackerman*'s undisputed facts established that NCMEC opened and viewed information other than the image that was the target of AOL's hash value match and "that AOL had not previously examined." *Id.* at 1306–07. NCMEC had exceeded, and did not merely repeat, AOL's private search and the Circuit thus held that NCMEC had violated the defendant's Fourth Amendment rights. *Id.*

But here, the facts differ. No evidence even suggests that NCMEC exceeded the scope of Sony's private search. Indeed, the logical inference the court draws from the undisputed facts is that NCMEC's review did not exceed Sony's private investigation. Mr. Meininger testified that

Sony does not use a hash value matching system. It follows that all of the information Sony sent NCMEC was first reviewed by a Sony employee. Mr. Meininger testified that the Sony Moderation Team "use[s] human eyes" to review every grief report it receives. So, when the Sony Moderators received the initial grief report about Susan_14 on June 6, 2012, a Sony Moderator opened the report and viewed the message and attached image. The court finds that NCMEC did not exceed the scope of Sony's private search when it reviewed Ms. Kawaguchi's August 8, 2012 report and found that it did not include child pornography.

Defendant also asserts that the government has not shown that the private search doctrine applies to other information Sony sent NCMEC—namely, the December 2012 and July 2013 image downloads. This is so, defendant argues, because the December 2012 downloads that Sony sent NCMEC were not the product of a new grief report, and the grief reports Sony received on July 25, 2013 did not contain any attached images. Defendant contends that because no one from Sony testified at the November 10, 2016 hearing about the extent of the reviews of these downloads by anyone from Sony before they were sent to NCMEC, the government cannot demonstrate that NCMEC did not exceed Sony's private search in December 2012 and July 2013.

But the government's circumstantial evidence makes defendant's conclusion an illogical one. In December 2012, Sony informed NCMEC that it had retrieved additional images from Susan_14 and those images warranted NCMEC's review. Sony then sent NCMEC more information it had retrieved from Susan_14's account. This submission included messages from Susan_14 seeking child pornography and images downloaded and stored on Susan_14's account. In July 2013, Sony sent NCMEC another report and attached two new images. Sony attached the images with its message "User's current photo downloads included the following: . . . ." Without

use of a filter like a hash value system, no one at Sony could have known about Susan_14's photos unless someone actually had "use[d] human eyes" to review them. In short, the court finds no evidence that NCMEC exceeded, rather than repeated, Sony's private search. The court thus concludes that the Fourth Amendment does not apply to NCMEC's subsequent search.

3. Reasonable Expectation of Privacy

Even if Sony acted as a government agent when it searched Susan_14's PSN account or NCMEC exceeded the scope of Sony's private search, the government contends that the Fourth Amendment does not apply because defendant lacked a reasonable expectation of privacy in the information. A search, for the purposes of the Fourth Amendment, occurs if there is "actual intrusion into a constitutionally protected area." *Kyllo v. United States*, 533 U.S. 27, 31 (2001). And an area is constitutionally protected against an unreasonable search only if "the individual manifested a subjective expectation of privacy in the object of the challenged search," and "society [is] willing to recognize that expectation as reasonable." *Id.* at 33 (quoting *California v. Ciraolo*, 476 U.S. 207, 211 (1986)). So, the test for determining whether a defendant had a reasonable expectation of privacy is two-fold. *United States v. Wells*, 739 F.3d 511, 518 (10th Cir. 2014). First, a defendant must have a subjective expectation of privacy. *Id.* Second, the defendant's expectation must be one "society would objectively consider reasonable." *Id.*

Defendant asserts that he had a subjective expectation of privacy in information that Sony sent to NCMEC. So, the question is whether defendant's subjective expectation of privacy in the evidence was objectively reasonable. The court divides this evidence into two categories for purposes of this analysis: (1) communications Susan_14 sent to other PSN users, and (2) image

downloads from Susan_14's account that Sony sent to NCMEC in December 2012 and July 2013.[2]

The government asserts that defendant had no objectively reasonable expectation of privacy in messages he sent from the Susan_14 account. The court agrees. Courts that have considered whether an individual has a reasonable expectation of privacy in electronic communications the individual has transmitted, generally treated electronic communications like mailed letters. And, while it is "well established that letters are 'in the general class of effects' protected by the Fourth Amendment . . . if a letter is sent to another, the sender's expectation of privacy ordinarily terminates upon delivery." *United States v. King*, 55 F.3d 1193, 1196 (6th Cir. 1995) (citation omitted); *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001) ("[The sender] would lose a legitimate expectation of privacy in an email that had already reached its recipient."). Defendant lost any reasonable expectation of privacy in his messages once they were delivered to the recipient. So, the Fourth Amendment does not apply to any communications that other PSN users received.

Whether defendant had a reasonable expectation of privacy in the image downloads from December 2012 and July 2013 is a more difficult question. Only recently have courts begun to consider whether the Fourth Amendment applies to an email when a user relies on an ISP to deliver and store it. *Ackerman*, 831 F.3d at 1305; *see also United States v. Forrester*, 512 F.3d 500, 510–11 (9th Cir. 2007) (finding no Fourth Amendment protection to the "to/from addresses of e-mail messages"); *United States v. Warshak*, 631 F.3d 266, 283–88 (6th Cir. 2010) (finding Fourth Amendment protection for email contents).

[2] Defendant also asserts that he had a reasonable expectation of privacy in data Sony turned over to the FBI on June 27, 2012—whatever that may be. But, from the parties' motions and the hearing on November 10, 2016, the court does not find that Sony turned over information to NCMEC on June 27, 2016.

In *United States v. Angevine*, the Tenth Circuit held that the defendant, then a professor at Oklahoma State University, had no reasonable expectation of privacy in data he downloaded from the internet onto the university's computers. 281 F.3d 1130, 1134 (10th Cir. 2002). "Within the workplace context, [the Supreme Court] has recognized that employees may have a reasonable expectation of privacy against intrusions by police." *Id.* (quoting *O'Connor v. Ortega*, 480 U.S. 709, 716 (1987)). But, the Tenth Circuit explained, public employees' expectations of privacy "may be reduced by . . . legitimate regulation." *Id.* Other factors the Tenth Circuit considers are: "(1) the employee's relationship to the item seized; (2) whether the item was in the immediate control of the employee when it was seized; and (3) whether the employee took actions to maintain his privacy in the item." *Id.*

The Tenth Circuit held that Oklahoma State University's policies and procedures prevented its employees from holding a reasonable expectation of privacy in data downloaded from the internet onto University computers. *Id.* The University's policy explicitly reserved the right to audit internet use randomly in its policy. *Id.* And the policy expressly warned that legal action might result if the employee's internet use violated federal law. *Id.* Also, the defendant's relationship to the University computer did not suggest a reasonable expectation of privacy because the University explicitly reserved the computer's ownership and data stored on it. *Id.* at 1134–35. The defendant was not in immediate control of the data when it was seized. *Id.* at 1135. So, by downloading child pornography through a monitored University computer network, the defendant did not take actions consistent with maintaining a privacy interest in the data. *Id.* Considering all relevant circumstances, the court determined that the defendant could not have held an objectively reasonable expectation of privacy in the data. *Id.*

The circumstances of this case do not involve the workplace or an employer/employee relationship. But the Tenth Circuit's analysis is instructive because the Circuit considered whether the employer's regulations reduced the employee's expectation of privacy. The same rationale applies to Sony and its PSN users. Here, Sony's policy explicitly nullified its users reasonable expectation of privacy. Before users could sign up for a PSN account, they had to agree to the Terms of Service Agreement. And the Terms of Service Agreement provides that Sony reserves the right to monitor "online activity on PSN." The agreement also warns users that they must not use the PSN to violate any local, state, or federal laws, and that any information Sony acquires while monitoring the users' activities may be turned over to appropriate law enforcement authorities. This agreement seemingly prevented defendant from having a reasonable expectation of privacy in information he stored on his PS3 device.

Defendant contends that the court should not construe Sony's Terms of Service Agreement to reduce his reasonable expectation of privacy because it is an adhesion contract. The court finds no merit in this argument. The Tenth Circuit has held that an adhesion contract is "a standardized contract offered by a transacting party with superior bargaining strength to a weaker party on a take-it-or-leave-it basis, without opportunity for bargaining." *THI of N. M. at Hobbs Ctr., LLC v. Spradlin*, 532 F. App'x 813, 818 (10th Cir. 2013). This kind of contract is "procedurally unconscionable and unenforceable when the terms are patently unfair to the weaker party." *Id.* And the party claiming unconscionability bears the burden to prove this affirmative defense. *Id.* But defendant has not demonstrated that the Terms of Service Agreement contains terms that are patently unfair to the weaker party. Defendant only asserts that no evidence exists that he "opened the user agreement or read its terms." Doc. 58 at 9. Defendant thus has not demonstrated that Sony's Terms of Service Agreement is an adhesion

contract. And, because the Terms of Service Agreement reduced defendant's reasonable expectation of privacy in the information stored on his PS3 device, the court finds that the Fourth Amendment does not apply to Sony's search of defendant's images.

B. Good Faith Exception

Alternatively, even if a Fourth Amendment violation occurred, the good faith exception to the Fourth Amendment's exclusionary rule applies here. This good faith exception is set forth in *United States v. Leon*, 468 U.S. 897 (1984). In *Leon*, the Supreme Court explained, "[i]f the purpose of the [Fourth Amendment's] exclusionary rule is to deter unlawful police conduct, then evidence obtained from a search should be suppressed only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment." 468 U.S. at 919 (quoting *United States v. Peltier*, 422 U.S. 531, 542 (1975)). The exclusionary rule serves to deter "deliberate, reckless, or grossly negligent conduct." *Herring v. United States*, 555 U.S. 135, 144 (2009). So, 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." *Id.*

The court finds no evidence of deliberate, reckless, or grossly negligent conduct by the police. When Agent Jones acquired a search warrant, she had no reason to believe that Sony had provided NCMEC with information procured in violation of defendant's Fourth Amendment rights. There was no evidence NCMEC had exceeded the scope of its authority when it relied on the information Sony provided. And, when the officers executed the search warrant on defendant's home, they had no reason to believe the warrant was obtained in violation of defendant's Fourth Amendment rights. When an officer relies on a warrant, a presumption exists

that the officer acts in good faith. *United States v. Cardall*, 773 F.2d 1128, 1133 (10th Cir. 1985); *see also Leon*, 468 U.S. at 922 ("[A] warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search." (internal quotation marks and citations omitted)).

In *Leon*, the Supreme Court described four scenarios where the exclusionary rule applies even though law enforcement secured a warrant. *Leon*, 468 U.S. at 914–23. None of them applies here. The first two of *Leon*'s four scenarios involve circumstances where the issuing magistrate issues the warrant based on a deliberately or recklessly false affidavit, or otherwise abandons his judicial role and fails to "perform his neutral and detached function." *Id.* at 914. Defendant presents no evidence that such facts exist here.

The third *Leon* scenario describes a situation where the warrant is based on an affidavit that is "so lacking in indicia of probable cause as to render official belief in its existence entirely questionable." *Id.* at 923. But the search warrant here was not supported by a bare bones affidavit. Agent Jones's affidavit relied on: (1) the two customer grief reports Sony received on July 25, 2013; (2) the PSN user profile for Susan_14; (3) Sony's past reports of account suspensions for Susan_14; (4) the photo downloads Sony had retrieved from Susan_14's account; (5) 10 archives Sony had downloaded from Susan_14's account; (6) results from the administrative subpoena served on Gmail seeking the email address: nudesusan14@gmail.com; and, (7) results from the administrative subpoena served on CenturyLink for the IP address 76.7.2.212.142 connected to nudesusan14@gmail.com, which linked this IP address to a Burlington, Kansas address. So, it was reasonable for the officers to believe that probable cause supported the warrant.

And last, *Leon* describes a scenario where the warrant was "so facially deficient" that it failed to particularize the place to be searched or the things to be seized. *Id*. No similar circumstances are present here.

Defendant also asserts that no evidence exists that a FBI or NCMEC employee acted in good faith reliance on any warrant (or settled case law) when they searched defendant's PSN content. Doc. 58 at 31–32. And, because Sony, NCMEC, and the FBI's warrantless searches formed the basis for Agent Jones's affidavit in support of the search warrant, the good faith exception does not apply. Defendant thus analogizes this case to *Murray v. United States*, 487 U.S. 533 (1988).

In *Murray*, officers illegally entered a warehouse and found contraband. 487 U.S. at 535–36. The officers then secured a warrant and reentered the warehouse. *Id.* The Supreme Court held that the evidence seized during the second search was not admissible if the officers' decision to seek the warrant was prompted by what the officers saw during the initial entry. *Id.* at 542. But the facts here differ, and the difference is a material one. The Supreme Court remanded *Murray* so the district court could determine whether probable cause from any source independent of the illegal search supported the warrant. *Id.* Here, the record already answers this question. The court has found no evidence derived from an illegal search. *See supra* A.1–2 (concluding no illegal search occurred in this case). Nor can the court find any evidence of bad faith. Agent Jones acted in good faith when she sought and secured the search warrant based on the information NCMEC sent her. And the law enforcement officers acted in good faith when they executed the search warrant on defendant's home.

In sum, even if a Fourth Amendment violation occurred, "the marginal or nonexistent benefits produced by suppressing evidence obtained" in the "objectively reasonable reliance on a

subsequently invalidated search warrant" cannot "justify the substantial costs of exclusion." *Leon*, 468 U.S. at 922. The court thus denies defendant's Motion.

IV. Conclusion

Defendant's Fourth Amendment rights were not violated. The court thus refuses to apply the exclusionary rule to suppress: (1) evidence NCMEC obtained from searching defendant's electronic communications; (2) evidence law enforcement officers acquired from searching defendant's residence; or, (3) statements defendant made to law enforcement during the search. The Fourth Amendment does not apply to Sony's search of defendant's information because Sony acted as a private entity. And, NCMEC, as a governmental entity, did not exceed the scope of Sony's private search. Even if Sony acted as a government agent when it searched defendant's information, the Fourth Amendment did not apply because defendant did not have a reasonable expectation of privacy in the information he stored on the PSN. Finally, even if defendant's Fourth Amendment rights were violated, the good faith exception applies and the exclusionary rule is not justified in this case.

IT IS THEREFORE ORDERED BY THE COURT THAT defendant's Motion to Suppress (Doc. 19) is denied.

IT IS SO ORDERED.

Dated this 17th day of January, 2017, at Topeka, Kansas.

s/ Daniel D. Crabtree
Daniel D. Crabtree
United States District Judge