



#30063-a-SRJ  
2023 S.D. 16

IN THE SUPREME COURT  
OF THE  
STATE OF SOUTH DAKOTA

\*\*\*\*

IN THE MATTER OF AN APPEAL BY AN  
IMPLICATED INDIVIDUAL

\*\*\*\*

APPEAL FROM THE CIRCUIT COURT OF  
THE SECOND JUDICIAL CIRCUIT  
MINNEHAHA COUNTY, SOUTH DAKOTA

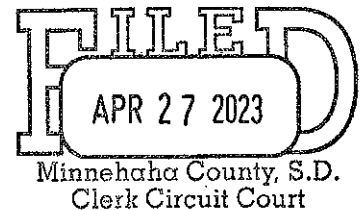
\*\*\*\*

THE HONORABLE JAMES A. POWER  
Judge

\*\*\*\*

STACY R. HEGGE of  
Gunderson, Palmer, Nelson &  
Ashmore, LLP  
Pierre, South Dakota

TALBOT J. WIECZOREK of  
Gunderson, Palmer, Nelson &  
Ashmore, LLP  
Rapid City, South Dakota



Attorneys for appellant  
Implicated Individual.

\*\*\*\*

STATE OF SOUTH DAKOTA  
In the Supreme Court  
I, Shirley A. Jameson-Fergel, Clerk of the Supreme Court of  
South Dakota, hereby certify that the within instrument is a true  
and correct copy of the original thereof as the same appears  
on record in my office. In witness whereof, I have hereunto set  
my hand and affixed the seal of said court at Pierre, S.D. this  
27<sup>th</sup> day of April, 2023.

Shirley A. Jameson-Fergel  
Clerk of Supreme Court  
Deputy

ARGUED  
MARCH 23, 2023  
OPINION FILED 04/05/23

PAUL S. SWEDLUND  
Solicitor General  
Pierre, South Dakota

Attorney for appellee State of  
South Dakota.

JEFFREY R. BECK  
Sioux Falls, South Dakota

Attorney for appellee  
ProPublica.

JON E. ARNESON  
Sioux Falls, South Dakota

Attorney for appellee Argus  
Leader.

JENSEN, Chief Justice

[¶1.] Following the completion of the State's criminal investigation involving T. Denny Sanford, also known as Implicated Individual,<sup>1</sup> the circuit court entered an order to unseal the search warrant affidavits related to the investigation. Sanford appeals, challenging the denial of his request to inspect and participate in redacting the affidavits before the circuit court unseals them. We affirm.

### Background

[¶2.] This is the second appeal by Sanford challenging the unsealing of a search warrant file containing five separate search warrants, returns of the warrants, inventories, and affidavits in an investigation involving Sanford. *See In re an Appeal by an Implicated Individual*, 2021 S.D. 61, 966 N.W.2d 578 (*Implicated Individual I*). In *Implicated Individual I*, the circuit court had initially sealed the entire search warrant file based upon law enforcement's representation that disclosure would impede the then-ongoing investigation. A ProPublica reporter requested the documents in the sealed file, prompting the circuit court to review the scope of its authority to seal the entirety of the search warrant file. ProPublica and intervenor Argus Leader (Press, collectively) submitted a joint brief to the circuit court arguing for the file to be unsealed. At the time, the State resisted unsealing the file, raising concerns that doing so would interfere with the investigation.

---

1. During the proceedings involved in the first appeal in *In re an Appeal by an Implicated Individual*, 2021 S.D. 61, 966 N.W.2d 578, T. Denny Sanford was referred to as Implicated Individual because his identity was not a matter of public record. The warrants were unsealed following our decision, and his identity is now a matter of public record.

#30063

Sanford also resisted the request, arguing that the release would impact his privacy and reputation.

[¶3.] Relying upon SDCL 23A-35-4.1, the circuit court issued amended orders providing that it was not authorized to seal the contents of the warrants, return of the warrants, or the inventories. The court ordered such “documents shall be unsealed and become publicly accessible court records.” The court concluded pursuant to SDCL 23A-35-4.1 that the affidavits in support of the five search warrants would remain sealed, but “[f]ollowing termination of the investigation or filing of an indictment, the document’s contents will [be] unsealed and available to public inspection or disclosure as a publicly accessible court record.” Sanford and the State appealed the orders, and the circuit court stayed its ruling pending appeal.

[¶4.] On appeal to this Court, Sanford argued that rules governing access to court records found in SDCL chapter 15-15A, promulgated by the South Dakota Supreme Court, conflicted with statutes enacted by the Legislature and must prevail because of the judiciary’s inherent authority over its records. *Implicated Individual I*, 2021 S.D. 61, ¶ 19, 966 N.W.2d at 584. We interpreted the plain language of SDCL 23A-35-4.1 to permit a circuit court to “seal the contents of an affidavit in support of a search warrant upon a showing of reasonable cause, but only until the investigation is terminated or an indictment or information is filed.” *Id.* ¶ 18, 966 N.W.2d at 583. We further observed that “[t]he statute’s text is equally clear in its command that the court ‘may not prohibit’ the public disclosure of other specific records, namely, the contents of the warrant, the return of the

warrant, and the inventory. Nor may the court prohibit public disclosure of the fact that a search warrant affidavit has been filed.” *Id.*

[¶5.] We emphasized that “a court’s discretion to ‘prohibit public access to information in a court record’” as set forth in SDCL 15-15A-13 is limited by the existence of “sufficient grounds to prohibit access *according to applicable constitutional, statutory and common law.*” *Id.* ¶ 21, 966 N.W.2d at 584 (quoting SDCL 15-15A-13).<sup>2</sup> We further noted, under SDCL 15-15A-8, that certain personally identifying information within court records must be redacted as a matter of course.<sup>3</sup> *Id.* ¶ 24, 966 N.W.2d at 585. While in *Implicated Individual I*

---

2. SDCL 15-15A-13 provides:

A request to prohibit public access to information in a court record may be made by any party to a case, the individual about whom information is present in the court record, or on the court’s own motion. Notice of the request must be provided to all parties in the case and the court may order notice be provided to others with an interest in the matter. The court shall hear any objections from other interested parties to the request to prohibit public access to information in the court record. The court must decide whether there are sufficient grounds to prohibit access according to applicable constitutional, statutory and common law. In deciding this the court should consider the purpose of this rule as set forth in § 15-15A-1. In restricting access, the court will use the least restrictive means that will achieve the purposes of this access rule and the needs of the requestor.

3. SDCL 15-15A-8 provides for automatic redaction of the following:

- (1) Social security numbers, employer or taxpayer identification numbers, and financial or medical account numbers of an individual.
- (2) Financial documents such as income tax returns, W-2’s and schedules, wage stubs, credit card statements, financial

(continued . . .)

#30063

there was “no redaction question before us[,]” we stated that “[w]e perceive no tension between our rules allowing for the limited redaction of this information to protect individual privacy interests and SDCL 23A-35-4.1’s requirement to allow access to the broader ‘contents’ of a search warrant.” *Id.*

[¶6.] Following our decision in *Implicated Individual I*, the Press filed with the circuit court a motion to unseal the affidavits and a motion to compel discovery on the status of the State’s investigation. The court denied the motion to unseal the affidavits because the State indicated the investigation was ongoing.

[¶7.] The State filed a notice of completed investigation with the circuit court on May 27, 2022, satisfying one of the triggering conditions upon which the circuit court’s amended orders required the affidavits to be unsealed. In response, Sanford filed a motion to stay the unsealing of the affidavits. He asserted a number of arguments in support of his claim, including: (1) that the Press was required to file a motion and make a showing supporting the unsealing of the affidavits; (2) that SDCL 23A-35-4.1 unconstitutionally violates rights of victims provided for in Article VI, § 29 of the South Dakota Constitution (Marsy’s Law); (3) that the absence of any court discretion under SDCL 23A-35-4.1 to stay the unsealing of the affidavits violated the presumption of innocence afforded to him by the Due Process Clause; (4) that certain comments by the media raised questions whether the State’s investigation had been completed; and (5) that Sanford should be provided access to

---

(... continued)

institution statements, check registers, and other financial information.

(3) The name of any minor child alleged to be the victim of a crime in any adult criminal proceeding.

#30063

the affidavits and allowed to participate in redaction before they are unsealed. The Press filed another motion to unseal the affidavits, arguing that the court had previously ordered the affidavits to be unsealed upon termination of the investigation while simultaneously arguing the inspection and redaction process proposed by Sanford was unnecessary.

[¶8.] On June 6, 2022, the circuit court denied Sanford's request to inspect the affidavits prior to their unsealing. In a June 16, 2022 order, the circuit court denied the motion to stay the unsealing of the affidavits and reiterated denial of the inspection request, finding that further delay would serve no valid purpose given the two years of litigation and ample opportunity for Sanford to have previously raised these issues.<sup>4</sup>

[¶9.] In ordering the affidavits to be unsealed, the circuit court concluded that nothing in SDCL 23A-35-4.1, this Court's interpretation of that statute in *Implicated Individual I*, or the circuit court's amended orders required the Press to make a formal request to unseal the affidavits. The court also rejected the Marsy's Law and Due Process constitutional claims as well as Sanford's argument that there were questions whether the State's investigation had concluded. Finally, the circuit court indicated its intent to redact "personally sensitive or identifying information, which in this case consists of personal email addresses, home addresses, phone numbers, and birth dates." The court noted that Sanford had not

---

4. The circuit court agreed to stay the order pending appeal. It found that further delay would substantially prejudice the Press because of the time-sensitive nature of the public interest in the investigation, however, and "gently remind[ed] the Implicated Individual and his counsel to remember the obligations imposed by Rule 11 as they contemplate[d] an appeal."



cited any authority that would require the court to permit the parties to participate in the redaction process or to extend the scope of redaction beyond personally identifying information in the affidavits.

[¶10.] Sanford raises a single issue on appeal:<sup>5</sup>

Whether the circuit court erred in denying Sanford's request to inspect the affidavits prior to their unsealing so that he may invoke his rights guaranteed by SDCL 15-15A-13.

### Analysis

#### *Standard of review.*

[¶11.] "Issues of constitutional and statutory interpretation are . . . subject to de novo review." *Thom v. Barnett*, 2021 S.D. 65, ¶ 13, 967 N.W.2d 261, 267 (citing *Jans v. Dep't of Pub. Safety*, 2021 S.D. 51, ¶ 10, 964 N.W.2d 749, 753). We also review the interpretation of our own court rules "de novo, utilizing our established rules for statutory construction." *Leighton v. Bennett*, 2019 S.D. 19, ¶ 7, 926 N.W.2d 465, 467–68. "Our standard of review for issues of statutory interpretation is well established." *Stanley v. Dep't of Pub. Safety*, 2023 S.D. 13, ¶ 10, \_\_\_ N.W.2d \_\_\_, \_\_\_. "[T]he language expressed in the statute is the paramount consideration' in statutory construction. Further, 'we give words their plain meaning and effect, and

---

5. On appeal, Sanford abandons the other arguments he made to the circuit court in opposing the unsealing of the affidavits. Interwoven within Sanford's inspection/redaction arguments, however, is a new claim that he has a Fourth Amendment privacy right in the investigative materials contained in the affidavits. The Fourth Amendment privacy right recognized in the cases cited by Sanford involved a challenge to the reasonableness of the search and seizure of property, not a privacy interest in the contents of the information that would be publicly disseminated in the search warrant affidavits. Sanford has failed to articulate a viable Fourth Amendment argument, and we determine this claim to be without merit.

#30063

read statutes as a whole.’ ‘When the language of a statute is clear, certain and unambiguous, there is no occasion for construction, and the court’s only function is to declare the meaning of the statute as clearly expressed in the statute.’” *Id.* (alteration in original) (quoting *Ibrahim v. Dep’t of Pub. Safety*, 2021 S.D. 17, ¶¶ 12–13, 956 N.W.2d 799, 802–03). Likewise, “[t]his [C]ourt assumes that court rules mean what they say[.]” *In re Yanni*, 2005 S.D. 59, ¶ 8, 697 N.W.2d 394, 398 (quoting *State v. Sorensen*, 1999 S.D. 84, ¶ 14, 597 N.W.2d 682, 684).

[¶12.] We have not previously addressed our standard of review for a court’s consideration under SDCL 15-15A-13 of a “request to prohibit public access to information in a court record . . . .” We conclude that a review under an abuse of discretion standard is appropriate. The circuit court’s order responding to Sanford’s request to view the affidavits and participate in redaction in advance of unsealing them is analogous to a request for a protective order relating to discovery, which we review for abuse of discretion. *In re Estate of Jones*, 2022 S.D. 9, ¶ 14, 970 N.W.2d 520, 526; *see also State v. Ralios*, 2010 S.D. 43, ¶ 47 n.4, 783 N.W.2d 647, 660 n.4 (in evidentiary context, “whether to redact and to what extent was within the sound discretion of the trial court”). “An abuse of discretion is ‘a fundamental error of judgment, a choice outside the reasonable range of permissible choices, a decision . . . [that], on full consideration, is arbitrary or unreasonable.’” *In re Estate of Jones*, 2022 S.D. 9, ¶ 14, 970 N.W.2d at 526 (alteration and omission in original) (quoting *Coester v. Waubay Twp.*, 2018 S.D. 24, ¶ 7, 909 N.W.2d 709, 711).

*Applicable statutory law.*

[¶13.] Sanford's appeal is based on his extrapolation of SDCL 15-15A-13, under which a party to a case may make "[a] request to prohibit public access to information in a court record . . . ." He argues that "[a]s a party to this matter and the subject of the court records, [Sanford] has requested a copy of the affidavits so that he may analyze them prior to their unsealing and invoke his rights under SDCL 15-15A-13 for redaction purposes if necessary." He thus attempts to frame this latest appeal as involving an entirely novel issue unresolved by *Implicated Individual I*. This case is no longer about the rules that apply to sealing the affidavits, he urges, but about the rules for redacting them upon their unsealing. He argues that for SDCL 15-15A-13 to be meaningful, the party challenging public access to information must be given an opportunity to inspect the records in order to make informed constitutional, statutory, and other legal objections to the public release of information contained in the affidavits and to provide input on appropriate redactions of the information.

[¶14.] Sanford also references SDCL 15-15A-7 (prohibiting public access to information excluded by federal or state law) and SDCL 15-15A-8 (prohibiting public access to certain information, such as social security numbers, financial information, and names of child victims) in support of his claims. Sanford contends that SDCL 23A-35-4.1 pertains to a *general* right of public access to search warrant records, whereas SDCL 15-15A-13 pertains to a *specific* prohibition against public access in certain circumstances.

#30063

[¶15.] The Press responds that Sanford's statutory claims are based upon the same arguments that this Court rejected in *Implicated Individual I*. The Press asserts that Sanford has not provided any substantive privacy right that would supplant the plain language of SDCL 23A-35-4.1 or the First Amendment right of the press and public to access the information contained in the affidavits.

[¶16.] The State also argues that the circuit court properly determined that the affidavits should be unsealed under SDCL 23A-35-4.1. The State highlights that the compelling interest it held in preventing public disclosure of the affidavits and facts underlying the investigation, as recognized by SDCL 23A-35-4.1, no longer exists now that the State has concluded its investigation. The State argues that requiring the unsealing of an affidavit, after the investigation has been completed, is consistent with "[s]ocietal interests in having law enforcement and the judiciary operate in the public eye [that are] not overcome simply because no indictment is returned. Society has as much interest in understanding why no indictment was returned as it does in understanding why one was." The State also rejects Sanford's claims that he should be permitted a special right of access to the sealed affidavits now that the investigation has been completed and the State has announced that charges will not be filed in South Dakota.

[¶17.] Sanford's reliance on SDCL 15-15A-13 to support his claim that the circuit court was required to stay the unsealing of the affidavits pending resolution of the inspection/redaction issue lacks support in the text of the rule and is irreconcilable with our decision in *Implicated Individual I*. SDCL 15-15A-13 simply provides a procedure for a party seeking "to prohibit public access to information in

#30063

a court record” when “there are sufficient grounds to prohibit access according to applicable constitutional, statutory and common law.” There is nothing in the language of SDCL 15-15A-13 that affords an affirmative or substantive privacy right to Sanford in the content of the affidavits. Nor does the rule forestall public access to the affidavits, as mandated by SDCL 23A-35-4.1, after the criminal investigation has been completed.<sup>6</sup>

[¶18.] Sanford’s effort to delay public access to the affidavits is also precluded by our decision in *Implicated Individual I*, where we stated that “[t]he plain language of [SDCL 23A-35-4.1] provides an unmistakable expression of legislative intent. A court may seal the contents of an affidavit in support of a search warrant upon a showing of reasonable cause, but only until the investigation is terminated or an indictment or information is filed.” 2021 S.D. 61, ¶ 18, 966 N.W.2d at 583. Further, in rejecting Sanford’s claim in *Implicated Individual I* that the provisions of SDCL chapter 15-15A supersede this statutory mandate, we stated:

The Legislature has enacted SDCL 23A-35-4.1, and nothing in our current rules conflicts with the statute’s provisions. To the contrary, our rules specifically contemplate the role of statutory authority in resolving questions concerning access to court records. We can no more overlook SDCL 23A-35-4.1 than we could ignore binding legal authority in this or any case that

---

6. The circuit court exhaustively reviewed the submissions of the parties in determining that the criminal investigation of Sanford had been completed, triggering the court’s obligation to unseal the search warrant affidavits under SDCL 23A-35-4.1. The court noted Sanford appeared to agree that the State had completed its investigation and concluded no crimes had been committed in South Dakota. The court observed the possibility of other states proceeding with a criminal investigation or prosecution but noted that neither party had informed the court of other pending investigations. On appeal, Sanford does not challenge the determination by the circuit court that the investigation had been completed.

comes before us.

*Id.* ¶ 27, 966 N.W.2d at 586.

[¶19.] Nonetheless, Sanford asks that we read SDCL 15-15A-13 to *require* the circuit court to allow inspection of the affidavits before they are unsealed to determine whether there may be confidential or sensitive information supporting redaction of some or all of the contents of the affidavits. There is nothing in SDCL 23A-35-4.1 or SDCL 15-15A-13 that mandates the circuit court to allow such an inspection. Moreover, we find no abuse of discretion in the court's decision to deny Sanford's request to inspect the affidavits and participate in the redaction of personal information before unsealing the affidavits.

[¶20.] In denying the request to review the affidavits, the circuit court determined that during the two years of litigation leading up to its current decision, Sanford had been afforded all the procedural protections set forth in SDCL 15-15A-13, requiring the court to "hear any objections from other interested parties to the request to prohibit public access to information in the court record[]" and to "decide whether there are sufficient grounds to prohibit access according to applicable constitutional, statutory and common law." Throughout the course of this litigation, the circuit court had the ability to review the information in the sealed affidavits and consider Sanford's privacy objections, as well as the statutory mandates in SDCL 23A-35-4.1. It is evident that the circuit court viewed Sanford's most recent motion as a belated and unpersuasive effort to further delay the unsealing of the affidavits required by statute.

#30063

[¶21.] Prior to ordering the affidavits unsealed, however, the court provided a thorough, well-reasoned decision denying Sanford's request to inspect the affidavits and participate in the routine redaction of certain personally identifying information. In considering Sanford's request to participate in the redaction process before unsealing the affidavits, the court determined that it was appropriate for the court, rather than Sanford, to redact any "personally identifying information," such as "personal email addresses, home addresses, phone numbers, and birth dates." In doing so, the court aptly expressed concerns that allowing the parties to participate in the redaction process would further extend the litigation and unnecessarily delay the unsealing of the affidavits required by SDCL 23A-35-4.1. The court also identified the greater potential for premature leaks of the information if the affidavits were provided to the parties. Finally, the court noted that the affidavits contained personally identifying information of others whose participation may also be required if the court granted Sanford's request. The court concluded that "each of these problems can be avoided if the [c]ourt and its staff simply make these redactions which they routinely and frequently make without participation by the interested parties."

[¶22.] The only significant change between *Implicated Individual I* and now is a factual one—the State has terminated its investigation, triggering the unsealing of the affidavits in support of search warrants under SDCL 23A-35-4.1 and the circuit court's amended court orders. The circuit court properly applied the provisions of SDCL 15-15A-13 and SDCL 23A-35-4.1 in considering, and ultimately denying, Sanford's request to inspect and redact the affidavits before they are

#30063

unsealed. Before ruling on the request, the court thoroughly considered the various statutory and constitutional grounds asserted by Sanford with respect to information that could conceivably be contained in the affidavits. The court's approach to redaction fell soundly within its discretion, and the court appropriately exercised its discretion to "decide whether there [were] sufficient grounds to prohibit access . . ." to contents of the affidavits under SDCL 15-15A-13.

[¶23.] Affirmed.

[¶24.] KERN, DEVANEY, and MYREN, Justices, and GILBERTSON, Retired Chief Justice, concur.

[¶25.] GILBERTSON, Retired Chief Justice, sitting for SALTER, Justice, who recused himself and did not participate in this matter.





STATE OF SOUTH DAKOTA )  
 : SS  
COUNTY OF MINNEHAHA )

IN CIRCUIT COURT  
SECOND JUDICIAL CIRCUIT

STATE OF SOUTH DAKOTA,  
Plaintiff,

-vs-

**AFFIDAVIT IN SUPPORT OF  
REQUEST FOR SEARCH  
WARRANT**

**THOMAS DENNY SANFORD**

██████████  
Defendant,

*JWA 19-911*

(In the matter of **Possession and Distribution of Child Pornography** in  
Minnehaha County, South Dakota)

\*\*\*\*\*  
The undersigned, being duly sworn upon oath, respectfully requests a Search  
Warrant to be issued for the following property:

**ITEMS TO BE SEARCHED FOR AND SEIZED:**

Oath Inc shall deliver to law enforcement the following records or  
information, in digital form (e.g. on CD/DVD), dating from January 1<sup>st</sup> 2019  
or opening of the AOL email account listed below to the time that this  
warrant is executed:

*AOL*  
*gk*  
Hotmail Email Account: ██████████

1. All business records and subscriber information, in any form kept,  
pertaining to the AOL email account listed above. Such information  
is to include but is not limited to the following:
  - a. Name, user identification number, and e-mail addresses
  - b. The subscriber birthday as listed
  - c. Profile contact information
  - d. Registered mobile number
  - e. Records of session times and durations
  - f. Date and time stamp of account creation
2. All electronic communications stored and presently contained in, or  
on behalf of the AOL email account listed above. Such information is  
to include but is not limited to the following:
  - a. All available read and unread incoming and outgoing email  
messages;
  - b. All available deleted email messages
  - c. All available draft email messages
  - d. All available saved email messages


- e. All available folder content
- 3. All transactional information and IP address connection logs associated with the AOL email account listed above. Such information is to include but is not limited to the following:
  - a. Connection time and date
  - b. Disconnect time and date
  - c. Method of connection to system (e.g., SLIP, PPP, Shell)
  - d. Data transfer volume (e.g., bytes)
  - e. The IP address or IP addresses associated with all connections and disconnections to and from the service
- 4. All user photos and other photos and images contained within the user account in original file format, including EXIF data and information;
- 5. All user videos, and other video files contained within the user account in original file format, including EXIF data and information.


**OATH INC IS PROHIBITED FROM NOTIFYING THE USER OF THE AOL EMAIL ADDRESS LISTED ABOVE OF THE EXISTANCE OF THE SEARCH WARRANT OR THAT THE SEARCH WARRANT HAD BEEN SERVED TO THE OATH INC. NOTIFICATION OF THE EXISTENCE OF THE SEARCH WARRANT TO THE USER OF THE EMAIL ACCOUNT LISTED ABOVE WOULD LIKELY RESULT IN THE LOSS AND/OR DISTRUCTION OF EVIDENCE AND WOULD IMPEDE THE ONGOING INVESTIGATIVE EFFORTS OF LAW ENFORCEMENT.**


The undersigned respectfully requests that the Search Warrant be issued to permit a search at the following premises for the above-described property:

The premises known as the offices of Oath Inc in the United States located at 22000 AOL Way Dulles, VA 20166 and all computer systems and digital storage contained within, accessible from or associated with Oath Inc regarding the following AOL email account: [REDACTED]

(PLACE INITIALS IN THE APPROPRIATE BLANK)

 Property that constitutes evidence of the commission of a criminal offense;

 Contraband, the fruits of a crime, or things otherwise criminally possessed:

 Property designed or intended for use in, or which is or has been used as the means of committing a criminal offense

The undersigned further requests:

(PLACE INITIALS IN THE APPROPRIATE BLANK)

\_\_\_\_\_ Execution of Search Warrant at night pursuant to SDCL 23A-35-4;

\_\_\_\_\_ That no notice be given prior to the execution of the Search Warrant pursuant to SDCL 23A-35-9;

\_\_\_\_\_ Authorization to serve the Search Warrant on Sunday;

 Execution of the Search Warrant during the daytime.

The facts in support of the issuance of a Search Warrant are as follows:

**Investigator Information:**

I, Jeff Kollars, am a Special Agent with the South Dakota Division of Criminal Investigation (DCI), Office of Attorney General for the State of South Dakota. As such, I am a state law enforcement officer responsible for the investigation of felony crimes committed in the State of South Dakota as required in SDCL 23-3-10. I am currently assigned to the Brookings, South Dakota DCI office and am responsible for conducting general criminal investigations in conjunction with, or independently from, local law enforcement. I have been assigned as a general crimes investigator for the DCI since May of 2013 and in that time have conducted investigations into all manner of criminal activity. This would include investigations into the offenses of rape, possession of child pornography, assault, theft, embezzlement, forgery, drug crimes, death investigations, and missing person cases.

I have been a sworn law enforcement officer in the State of South Dakota since May of 2006 and was employed as a State Trooper with the SD Highway Patrol from 2005 to 2013. I have received specialized training in interviewing and interrogation, crime scene processing, evidence collection, sexual assault investigation, electronic crimes and homicide investigation. I have conducted numerous interviews with individuals suspected of committing all manner of crimes. I hold a bachelor's of science degree in Criminal Justice from the University of South Dakota in Vermillion, SD.

I am familiar with the facts and circumstances described herein and make this affidavit based upon personal knowledge derived from my participation in this investigation, conclusions I have reached based on my training and experience, and upon information I believe to be reliable from oral and written reports about this investigation and other investigations which I have received from state or local law enforcement officers from other law enforcement agencies.

**Current Investigation:**

On August 14<sup>th</sup> 2019, the National Center for Missing and Exploited Children (NCMEC) sent a CyberTip to the South Dakota Internet Crimes Against Children (ICAC) Task Force. The CyberTip had been submitted to NCMEC by Oath Inc, Inc. on July 9<sup>th</sup> 2019. The CyberTip was regarding a AOL/ Oath Inc user account that contained image files that were suspected of depicting child pornography and child erotica. On August 15<sup>th</sup> 2019 the CyberTip was assigned to me for

investigation.

Based upon my training, knowledge and experience, I know that AOL was merged with Yahoo.com into what is now called Oath Inc. Oath Inc. is a Verizon Communications Company. Oath Inc provides a law enforcement contact address of 22000 AOL Way Dulles, VA 20166. AOL has a range of integrated products for members including communication tools, mobile apps and services and subscription packages. It provides dial up internet access, AOL mail, AOL instant messenger and AOL Desktop which is a internet suite integrating a web browser, media player and instant messenger.

Upon review of the information that was contained in the CyberTip, I learned that on July 9<sup>th</sup> 2019 AOL / Oath Inc. discovered 36 image files contained within a AOL user account that was suspected of depicting child pornography.

The information provided by Oath, Inc. in the CyberTip indicated that the name for the AOL account in question was Denny Sanford with a phone number of [REDACTED]. The reported email address was [REDACTED]. A user name of VEJ6VUOXNEO4D3EFGW7IORXFDU-aol was listed for the account. There was also an alternate email address of [REDACTED] reported.

Next, I reviewed the images reported to me from Oath Inc in the cybertip. The 36 images were three separate unique images, repeated several times. The first image was identified as 129055062\_image.63-1.jpeg being a juvenile female standing nude facing the camera. Her breasts and vagina were visible in the image. In the back ground was some green foliage and white drapes. Her right hand is on her right hip. The estimated age of the female is 12 to 15 years old.

The second image that was also repeated is identified as 129055094\_image.89-1.jpeg. It can be described as a nude juvenile female standing facing the camera. Her breasts and vagina are visible in the image. There is snow in the background and her hair is brown. The estimated age of the juvenile is 8 to 12 years old.

The third image is 129055159\_image.65-1.jpeg and is also repeated several times. The image can be described as a nude juvenile female standing, facing the camera. Her left hand is near her mouth and right hand on her abdomen. There is green foliage visible in the back ground. The estimated age of the female is 10 to 15 years old.

On September 3<sup>rd</sup> 2019, I received a subpoena from the Brookings County States Attorney requesting account registration information for the Verizon phone number [REDACTED]. I later received a report back from Verizon identifying the account being registered to Premier BankCard LLC effective from 3/5/2013 to present with a contact name of Dana Anthony (address of [REDACTED]).

Sioux Falls, SD).

I made several attempts to contact Dana Anthony with Premier Bank and was able to have a phone conversation with her on November 20<sup>th</sup> 2019. In the conversation, she first told me that no one at the bank had the number listed above. She then told me that the number was used by Denny Sanford. She also provided me with his personal assistant, Cobyann Berglund's contact information [REDACTED]

On November 20<sup>th</sup> 2019, I received a phone call from Attorney Marty Jackley who informed me that he was representing Denny Sanford and Premiere Bank. He stated that he anticipates cooperating with law enforcement but requested that all further communication go through him.

I also received subpoenas from the Brookings County States Attorney for account registration information for [REDACTED] and [REDACTED] from Oath Inc. The subpoenas were served and information later provided by Oath identifying [REDACTED] as being registered to Denny Sanford and an associated email of [REDACTED] and phone number of [REDACTED] (verified). The account was listed as terminated and created on November 12, 1997.

The returned information from Oath Inc. provided account registration for [REDACTED] as being registered to Cobyann Berglund with phone numbers [REDACTED] and [REDACTED] being associated with the account. The account was created November 12<sup>th</sup> 1997 and was listed as active.

I also served a subpoena to Brookings Municipal Utilities (BMU) for the number [REDACTED] which was listed as being associated with BMU in the Cybertip in a search. On November 29<sup>th</sup> 2019, I was informed by representatives from BMU that they had no record of a account with that number.

I also conducted a driver license search in South Dakota of Denny Sanford in which I found an active driver license of Thomas Denny Sanford DOB: [REDACTED] with an address of [REDACTED]

I also conducted a web search of the name Denny Sanford which provided multiple records identifying Thomas Denny Sanford as a South Dakota business man and philanthropist who was the founder of First Premier Bank and the CEO of its holding company, United National Corporation.

Based on the information listed above it appears likely that the AOL account of [REDACTED] was being operated by Thomas Denny Sanford during the time that Oath, Inc. discovered the image file suspected of depicting child pornography.

**The affiant wishes to draw the court's attention to the following facts regarding inferences from the above mentioned facts that are based upon my knowledge, training and experience:**

Based on my training and experience, I know that it is common for users of email accounts to keep and store both incoming and outgoing email messages as well as draft email messages and deleted email messages within their email accounts.

Based upon my training and experience, I know that individuals involved in acts of child sexual exploitation including the manufacture, possession and distribution of child pornography may use various mechanisms to communicate with other offenders, including communications through various email accounts. Your affiant is aware that individuals involved in criminal activity may mask their identity and use a false alias. Your affiant is further aware that individuals involved in acts of child sexual exploitation including child pornography may create electronic accounts including e-mail accounts with false aliases to further their ability to communicate with other offenders and/or victims.

Based upon my training and experience, I know that individuals who use the Internet for the manufacture, possession or distribution of child pornography will often times keep or store images of minors engaging in prohibited sexual acts. These individuals will sometimes use various e-mail accounts to store the images of minors engaging in prohibited sexual acts.

Based upon my training and experience, I know that electronic and/or written communication may exist within an e-mail account or elsewhere, demonstrating the access to child pornography and/or child sexual exploitation.

Based on my training and experience, I know that Electronic Service Providers who offer web-based email accounts often times store and maintain user content within their computer systems and computer servers. This user content often times includes the entire contents of a user's email account including subscriber information, IP address logs, connection logs along with actual email messages and email content. This user content is typically stored within computer systems, computer servers and other forms of digital storage owned and/or maintained by the Electronic Service Provider.

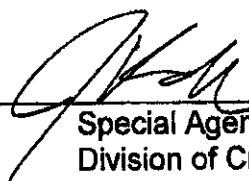
Based upon my training and experience, I know that many email providers and Electronic Service Providers do not monitor the content of messages being exchanged by users. Therefore, individuals who are involved with the possession of child pornography will often times use email accounts to communicate with victims or exchange contraband and illicit material with other individuals.

Based upon my training and experience, I know that it is the policy of Oath Inc to notify users about legal process that has been served in relation to the user's


account. However, I also know that Microsoft will not notify user's about legal process where prohibited by law and/or court order. Therefore, I am requesting that Oath Inc be prohibited from notifying the user of the email account with the email address of [REDACTED] of the existence of this legal process. I believed that if notification is given to the user it would likely result in the loss and/or destruction of evidence and would impede the ongoing investigative efforts of law enforcement.

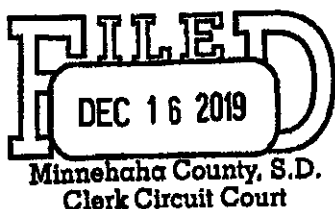
Based upon the information described above, I have probable cause to believe that on the computer systems owned, maintained, and/or operated by the company known as Oath Inc in the United States, 22000 AOL Way Dulles, VA 20166, there exists evidence, fruits, and instrumentalities of violations of state and/or federal law. By this Affidavit and application, I respectfully request that the Court issue a search warrant directed to Oath Inc, allowing agents to seize the electronic communications and other information stored on Oath Inc /AOL computer systems and computer servers for the AOL e-mail account of [REDACTED] and the associated files described above.

For these reasons, I request authority to seize all electronic communications and other content stored in the Target Account, to be searched off-site in a controlled environment. Law enforcement officers and agents will review the records sought by the search warrant and will segregate any messages and content constituting evidence, fruits or instrumentalities of violations of state and/or federal criminal law. Additionally, I request authority to serve the warrant on the Microsoft Corporation by facsimile and to allow Oath Inc to copy the data outside of this officer's presence.

  
Special Agent Jeff Kollars  
Division of Criminal Investigation

Subscribed and sworn to before me this 9<sup>th</sup> day of December, 2019.

  
\_\_\_\_\_  
(Notary Public)  
My commission expires 9/15/23





STATE OF SOUTH DAKOTA )  
 : SS  
COUNTY OF MINNEHAHA )  
\*\*\*\*\*

IN CIRCUIT COURT  
SECOND JUDICIAL CIRCUIT  
\*\*\*\*\*

STATE OF SOUTH DAKOTA,  
Plaintiff,  
-vs-

**AFFIDAVIT IN SUPPORT OF  
REQUEST FOR SEARCH  
WARRANT**

**THOMAS DENNY SANFORD**  
DOB: [REDACTED]  
Defendant,

*JWA 20-402*

(In the matter of **Possession and Distribution of Child Pornography** in Minnehaha County, South Dakota)

\*\*\*\*\*  
The undersigned, being duly sworn upon oath, respectfully requests a Search Warrant to be issued for the following property:

**ITEMS TO BE SEARCHED FOR AND SEIZED:**

Midcontinent Communications (Midco) shall deliver to law enforcement the following records or information, in digital form (e.g. text file ".txt", document file ".doc" or Portable Document Format ".pdf"), regarding the IP addresses of:

2001:48f8:72:7e1:791c:a1d1:7233:c38 on June 27<sup>th</sup> 2019 at 18:33:02 hours UTC and 18:32:55 hours UTC

1. All business records and subscriber information, in any form kept, pertaining to the IP address listed above. Such information is to include but is not limited the following:
  - a. Subscriber name;
  - b. Subscriber address;
  - c. Subscriber phone number;
  - d. All screen names and/or email addresses;
  - e. Status of account;
  - f. Detailed billing logs;
  - g. Date account was created and if applicable, date account was closed;
  - h. Method of payment;
  - i. Detailed billing records
  
2. All transactional information and IP address connection logs associated with the subscriber of IP address listed above. Such information is to include but is not limited to the following:
  - a. Connection time and date;
  - b. Disconnect time and date;
  - c. Method of connection to system (e.g., SLIP, PPP, Shell);
  - d. Device information for each connection.

The undersigned respectfully requests that the Search Warrant be issued to permit a search at the following premises for the above-described property:

**The premises known as the offices of Midcontinent Communications (Midco) in the United States located at 3901 N Louise Avenue, Sioux Falls, SD 57107 and all computer systems and digital storage contained within, accessible from or associated with Midcontinent Communications (Midco) regarding the following IP address:**

**2001:48f8:72:7e1:791c:a1d1:7233:c38 on June 27<sup>th</sup> 2019 at 18:33:02 hours UTC and 18:32:55 hours UTC**

**MIDCONTINENT COMMUNICATIONS (MIDCO) IS PROHIBITED FROM NOTIFYING THE USER OF THE IP ADDRESS, EMAIL ADDRESS LISTED ABOVE OF THE EXISTENCE OF THE SEARCH WARRANT OR THAT THE SEARCH WARRANT HAD BEEN SERVED TO MIDCONTINENT COMMUNICATIONS (MIDCO). NOTIFICATION OF THE EXISTENCE OF THE SEARCH WARRANT TO THE USER OF THE ACCOUNT LISTED ABOVE WOULD LIKELY RESULT IN THE LOSS AND/OR DESTRUCTION OF EVIDENCE AND WOULD IMPEDE THE ONGOING INVESTIGATIVE EFFORTS OF LAW ENFORCEMENT.**

(PLACE INITIALS IN THE APPROPRIATE BLANK)

- Property that constitutes evidence of the commission of a criminal offense;
- Contraband, the fruits of a crime, or things otherwise criminally possessed;
- Property designed or intended for use in, or which is or has been used as the means of committing a criminal offense

The undersigned further requests:

(PLACE INITIALS IN THE APPROPRIATE BLANK)

- Execution of Search Warrant at night pursuant to SDCL 23A-35-4;
- That no notice be given prior to the execution of the Search Warrant pursuant to SDCL 23A-35-9;
- Authorization to serve the Search Warrant on Sunday;
- Execution of the Search Warrant during the daytime.

The facts in support of the issuance of a Search Warrant are as follows:

**Investigator Information:**

I, Jeff Kollars, am a Special Agent with the South Dakota Division of Criminal Investigation (DCI), Office of Attorney General for the State of South Dakota. As such, I am a state law enforcement officer responsible for the investigation of felony crimes committed in the State of South Dakota as required in SDCL 23-3-10. I am currently

assigned to the Brookings, South Dakota DCI office and am responsible for conducting general criminal investigations in conjunction with, or independently from, local law enforcement. I have been assigned as a general crimes investigator for the DCI since May of 2013 and in that time have conducted investigations into all manner of criminal activity. This would include investigations into the offenses of rape, possession of child pornography, assault, theft, embezzlement, forgery, drug crimes, death investigations, and missing person cases.

I have been a sworn law enforcement officer in the State of South Dakota since May of 2006 and was employed as a State Trooper with the SD Highway Patrol from 2005 to 2013. I have received specialized training in interviewing and interrogation, crime scene processing, evidence collection, sexual assault investigation, electronic crimes and homicide investigation. I have conducted numerous investigations with individuals suspected of committing all manner of crimes. I hold a bachelor's of science degree in Criminal Justice from the University of South Dakota in Vermillion, SD.

I am familiar with the facts and circumstances described herein and make this affidavit based upon personal knowledge derived from my participation in this investigation, conclusions I have reached based on my training and experience, and upon information I believe to be reliable from oral and written reports about this investigation and other investigations which I have received from state or local law enforcement officers from other law enforcement agencies.

**Current Investigation:**

On August 14<sup>th</sup> 2019, the National Center for Missing and Exploited Children (NCMEC) sent a Cyber Tip to the South Dakota Internet Crimes Against Children (ICAC) Task Force. The Cyber Tip had been submitted to NCMEC by Oath Inc, Inc. on July 9<sup>th</sup> 2019. The Cyber Tip was regarding an AOL/ Oath Inc user account that contained image files that were suspected of depicting child pornography and child erotica. On August 15<sup>th</sup> 2019 the CyberTip was assigned to me for investigation.

Based upon my training, knowledge and experience, I know that AOL was merged with Yahoo.com into what is now called Oath Inc. Oath Inc. is a Verizon Communications Company. Oath Inc provides a law enforcement contact address of 22000 AOL Way Dulles, VA 20166. AOL has a range of integrated products for members including communication tools, mobile apps and services and subscription packages. It provides dial up internet access, AOL mail, AOL instant messenger and AOL Desktop which is an internet suite integrating a web browser, media player and instant messenger.

Upon review of the information that was contained in the CyberTip, I learned that on July 9<sup>th</sup> 2019 AOL / Oath Inc. discovered 36 image files contained within a AOL user account that was suspected of depicting child pornography.

The information provided by Oath, Inc. in the Cyber Tip indicated that the name for the AOL account in question was Denny Sanford with a phone number of [REDACTED]. The reported email address was [REDACTED]. A username of VEJ6VUOXNEO4D3EFGW7IORXFDU-aol was listed for the account. There was also an alternate email address of [REDACTED] reported.

Next, I reviewed the images reported to me from Oath Inc in the cyber tip. The 36

images were three separate unique images, repeated several times. The first image was identified as 129055062\_image.63-1.jpeg being a juvenile female standing nude facing the camera. Her breasts and vagina were visible in the image. In the background was some green foliage and white drapes. Her right hand is on her right hip. The estimated age of the female is 12 to 15 years old.

The second image that was also repeated is identified as 129055094\_image.89-1.jpeg. It can be described as a nude juvenile female standing facing the camera. Her breasts and vagina are visible in the image. There is snow in the background and her hair is brown. The estimated age of the juvenile is 8 to 12 years old.

The third image is 129055159\_image.65-1.jpeg and is also repeated several times. The image can be described as a nude juvenile female standing, facing the camera. Her left hand is near her mouth and right hand on her abdomen. In the image, her right breast is visible along with her vagina. There is green foliage visible in the background. The estimated age of the female is 10 to 15 years old.

On September 3<sup>rd</sup> 2019, I received a subpoena from the Brookings County States Attorney requesting account registration information for the Verizon phone number [REDACTED]. I later received a report back from Verizon identifying the account being registered to Premier BankCard LLC effective from 3/5/2013 to present with a contact name of Dana Anthony (address of [REDACTED]).

I made several attempts to contact Dana Anthony with Premier Bank and was able to have a phone conversation with her on November 20<sup>th</sup> 2019. In the conversation, she first told me that no one at the bank had the number listed above. She then told me that the number was used by Denny Sanford. She also provided me with his personal assistant, Cobyann Berglund's contact information [REDACTED].

On November 20<sup>th</sup> 2019, I received a phone call from Attorney Marty Jackley who informed me that he was representing Denny Sanford and Premiere Bank. He stated that he anticipates cooperating with law enforcement but requested that all further communication go through him.

I also received subpoenas from the Brookings County States Attorney for account registration information for [REDACTED] and [REDACTED] from Oath Inc. The subpoenas were served and information later provided by Oath identifying [REDACTED] as being registered to Denny Sanford and an associated email of [REDACTED] and phone number of [REDACTED] (verified). The account was listed as terminated and created on November 12, 1997.

The returned information from Oath Inc. provided account registration for [REDACTED] as being registered to Cobyann Berglund with phone numbers [REDACTED] and [REDACTED] being associated with the account. The account was created November 12<sup>th</sup> 1997 and was listed as active.

For clarification purposes, I also served a subpoena to Brookings Municipal Utilities (BMU) for the number [REDACTED] which was listed as being associated with BMU in the Cyber tip from a search that they had completed. On November 29<sup>th</sup> 2019, I was informed by representatives from BMU that they had no record of a account with that number at any point.

I also conducted a driver license search in South Dakota of Denny Sanford in which I found an active driver license of Thomas Denny Sanford DOB: [REDACTED] with an address of [REDACTED] and a mailing address of [REDACTED]

I also conducted a web search of the name Denny Sanford which provided multiple records identifying Thomas Denny Sanford as a South Dakota businessman and philanthropist who was the founder of First Premier Bank and the CEO of its holding company, United National Corporation.

On December 9<sup>th</sup> 2020, I produced a affidavit in support of a search warrant for Oath Inc records and content of the email address [REDACTED]. The search warrant was presented to the Honorable Judge James Power of the 2<sup>nd</sup> Circuit in Sioux Falls, SD who later signed the warrant. I later served the warrant on Oath Inc.

On January 10<sup>th</sup> 2020, I received the account records including emails from Oath Inc. for [REDACTED] pursuant to the warrant mentioned above. In review of the content I observed the following emails:

- 1) Email from [REDACTED] to [REDACTED]
  - a. Sent: May 28<sup>th</sup>, 2019 4:48:59 PM UTC
  - b. With the signature line saying "Sent from my Verizon Samsung Galaxy smartphone"
  - c. Including one picture attachment identified as file name 20190528\_092836.jpg
  - d. A description of this the image 20190528\_092836.jpg is described by myself as follows: The image is of a prepubescent female laying on her back, completely nude. Her vagina is visible on the left portion of the image with her legs spread. Her right breast is visible, and her face is on the right side of the image. There is a portion of blue material visible in the upper right portion of the photograph. There are several lines of deviation visible making the image appear to be a picture taken of another screen.
  
- 2) Email from [REDACTED] to [REDACTED]
  - a. Sent May 29<sup>th</sup>, 2019 1:39:09 PM UTC
  - b. With the signature line saying "Sent from my Verizon Samsung Galaxy smartphone"
  - c. Including one picture attachment identified as file name 20190528\_092836.jpg
  - d. The image appears to be the exact same image as identified above (#1).
  
- 3) Email from [REDACTED] to [REDACTED]
  - a. Sent June 27<sup>th</sup>, 2019 12:33:02 PM UTC

- b. The subject line is "Emailing: 0\_270" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:

0\_270

Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.

- c. Including one picture attachment identified as file name 0\_270.jpg.
- d. A description of this the image 0\_270.jpg is described by myself as follows: a juvenile female standing nude facing the camera. Her breasts and vagina are visible in the image. In the background was some green foliage and white drapes. Her right hand is on her right hip. The estimated age of the female is 12 to 15 years old. This image appears to be the same image described above as the first image within the MCMEC cyber tip.

4) Email from [REDACTED] to [REDACTED]

- a. Sent June 27<sup>th</sup>, 2019 12:34:04 PM UTC.

- b. The subject line is "Emailing: 0\_735" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:

0\_735

Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.

- c. Including one picture attachment identified as file name 0\_735.jpg
- d. A description of this the image 0\_735.jpg is described by myself as follows: a juvenile female standing nude facing the camera. She has blonde chest high straight hair which is down. Her right arm is crossing her chest and is resting on her left shoulder. Her left arm is resting on her right hip. Her vagina and both breasts are visible. The background of the photograph has a body of water and the ground around her is grassy. Her estimated age is 10 to 14 years of age.

5) Email from [REDACTED] to [REDACTED]

- a. Sent June 27<sup>th</sup>, 2019 12:34:46 PM UTC.

- b. The subject line is "Emailing: 0\_189" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:

0\_189

Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.

- c. Including one picture attachment identified as file name 0\_189.jpg

- d. A description of this the image 0\_189.jpg is described by myself as follows: It can be described as a nude juvenile female standing facing the camera. Her breasts and vagina are visible in the image. There is snow in the background and her hair is brown. The estimated age of the juvenile is 8 to 12 years old. This image is the second image described above within the MCMEC cyber tip.
- 6) Email from [REDACTED] to [REDACTED]
- a. Sent June 27<sup>th</sup>, 2019 5:47:00 PM UTC.
  - b. The subject line is "Emailing: 0\_588" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:  
0\_588  
Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.
  - c. Including one picture attachment identified as file name 0\_588.jpg
  - d. A description of the image 0\_588.jpg is that of a nude juvenile female standing, facing the camera. Her left hand is near her mouth and right hand on her abdomen. There is green foliage visible in the background. The estimated age of the female is 10 to 15 years old. This image is the third image described above within the MCMEC cybertip.
- 7) Email from [REDACTED] to [REDACTED]
- a. Sent June 27<sup>th</sup>, 2019 5:47:37 PM UTC
  - b. The subject line is "Emailing: 0\_270" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:  
0\_270  
Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.
  - c. Including one picture attachment identified as file name 0\_270.jpg.
  - d. A description of this the image 0\_270.jpg is the same as listed above in number "3" and appears to be the same image sent again.
- 8) Email from [REDACTED] to [REDACTED]
- a. Sent June 27<sup>th</sup>, 2019 6:34:28 PM UTC
  - b. The subject line is "Emailing: 0\_270" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:  
0\_270

Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.

- c. Including one picture attachment identified as file name 0\_270.jpg.
- d. A description of this the image 0\_270.jpg is the same as listed above in number "3" and appears to be the same image sent again.

Based on my training and experience and all the information relied upon in this investigation, I feel that the content of the image files described above fit the definition of child pornography as described in South Dakota Codified Law and fit well within definition and section SDCL 22-24A-3:

*a. Possessing, manufacturing, or distributing child pornography--Felonies--Assessment. A person is guilty of possessing, manufacturing, or distributing child pornography if the person:*

- (1) Creates any visual depiction of a minor engaging in a prohibited sexual act, or in the simulation of such an act;*
- (2) Causes or knowingly permits the creation of any visual depiction of a minor engaged in a prohibited sexual act, or in the simulation of such an act; or*
- (3) Knowingly possesses, distributes, or otherwise disseminates any visual depiction of a minor engaging in a prohibited sexual act, or in the simulation of such an act.*

*Consent to performing these proscribed acts by a minor or a minor's parent, guardian, or custodian, or mistake as to the minor's age is not a defense to a charge of violating this section.*

*A violation of this section is a Class 4 felony. If a person is convicted of a second or subsequent violation of this section within fifteen years of the prior conviction, the violation is a Class 3 felony.*

*The court shall order an assessment pursuant to § 22-22-1.3 of any person convicted of violating this section.*

*b. "Prohibited sexual act," actual or simulated sexual intercourse, sadism, masochism, sexual bestiality, incest, masturbation, or sadomasochistic abuse; actual or simulated exhibition of the genitals, the pubic or rectal area, or the bare feminine breasts, in a lewd or lascivious manner; actual physical contact with a person's clothed or unclothed genitals, pubic area, buttocks, or, if such person is a female, breast with the intent to arouse or gratify the sexual desire of either party; defecation or urination for the purpose of creating sexual excitement in the viewer; or any act or conduct which constitutes sexual battery or simulates that sexual battery is being or will be committed. The term includes encouraging, aiding, abetting or enticing any person to commit any such acts as provided in this subdivision. The term does not include a mother's breast-feeding of her baby;*

In review of the same emails included in the [REDACTED] account, several of the emails within the account include identifiers such as a photograph of a South Dakota Driver license of Thomas Denny Sanford DOB [REDACTED] with a physical address of [REDACTED] sent via email on 4/29/2019 via [REDACTED]



A letter from The Dalai Lama to T. Denny Sanford thanking him for support for a University of California San Diego T. Denny Sanford Institute for Empathy and Compassion dated 6/11/2019 sent from [REDACTED].

A photograph of a hotel receipt from the Curio Collection by Hilton of Coronado, California with a one night stay on February 9<sup>th</sup> 2019 and a guest name of Denny Sanford sent to email address [REDACTED] on February 6<sup>th</sup> 2019.

There were several photographs of a person that I believe to be Denny Sanford in a hospital gown, in an airplane, and sitting at a table. There were also photographs of decorative windows from Sanford Hospital in Sioux Falls, SD.


The same records received from Oath Inc on January 10<sup>th</sup> 2020 for [REDACTED] included log in data with IP addresses from May 28<sup>th</sup> and 29<sup>th</sup> 2019 and also June 27<sup>th</sup> 2020.

I conducted Internet Service Provider (ISP) lookups regarding all of the IP addresses.

The IP addresses for May 28<sup>th</sup> and 29<sup>th</sup> 2019 and June 27<sup>th</sup>, 2019 and corresponding providers are as follows:

<u>Email address</u>	<u>IP</u>	<u>Date</u>	<u>Provider</u>
	174.213.18.4	May 30 2019 04:10:59	Verizon wireless
	52.34.110.242	May 29 2019 23:15:11	Amazon
	52.24.183.101	May 29 2019 23:13:03	Amazon
	54.190.199.109	May 29 2019 23:13:02	Amazon
	2001:579:84a0:7:e1b7:e997:dd64:50d1	May 29 2019 23:13:01	Cox Communication
	76.176.201.7	May 29 2019 23:10:59	Spectrum
	76.176.201.7	May 29 2019 23:01:18	Spectrum
	52.24.183.101	May 29 2019 22:54:52	Amazon
	52.34.110.242	May 29 2019 22:54:49	Amazon
	76.176.201.7	May 29 2019 22:54:47	Spectrum
	76.176.201.7	May 29 2019 22:54:44	Spectrum
	174.213.5.179	May 29 2019 21:11:00	Verizon wireless
	2600:1012:b15d:bb5f:9c37:a043:93db:30d0	May 29 2019 20:50:59	Verizon wireless
	174.213.5.179	May 29 2019 20:19:39	Verizon wireless
	174.212.21.98	May 29 2019 18:10:59	Verizon wireless
	34.221.128.86	May 29 2019 16:46:43	Amazon
	76.176.201.7	May 29 2019 15:18:15	Spectrum
	2600:1012:b100:bb44:6998:c8dd:f2e:96ae	May 29 2019 04:49:55	Verizon wireless
	174.212.9.9	May 29 2019 04:10:59	Verizon wireless
	2600:1012:b100:bb44:6998:c8dd:f2e:96ae	May 28 2019 23:24:52	Verizon wireless
	52.24.183.101	May 28 2019 23:11:53	Amazon
	54.191.16.110	May 28 2019 23:11:52	Amazon
	2001:579:84a0:7:3c42:625e:6757:442	May 28 2019 23:11:51	Cox Communication
	174.212.9.9	May 28 2019 23:11:00	Verizon wireless
	2600:1012:b16b:c79c:7c14:e651:2f51:286a	May 28 2019 22:14:48	Verizon wireless
	76.176.201.7	May 28 2019 21:24:43	Spectrum
	76.176.201.7	May 28 2019 21:12:13	Spectrum
	76.176.201.7	May 28 2019 21:10:59	Spectrum
	52.24.183.101	May 28 2019 18:45:46	Amazon
	52.34.110.242	May 28 2019 18:45:42	Amazon
	76.176.201.7	May 28 2019 18:45:41	Spectrum
	76.176.201.7	May 28 2019 18:45:37	Spectrum
	18.237.215.236	May 28 2019 17:54:02	Amazon
	76.176.201.7	May 28 2019 17:54:01	Spectrum
	76.176.201.7	May 28 2019 17:30:52	Spectrum
	52.34.110.242	May 28 2019 16:29:48	Amazon
	34.221.128.86	May 28 2019 16:25:08	Amazon
	174.213.9.175	May 28 2019 05:14:07	Verizon wireless
	174.213.9.175	May 28 2019 05:11:08	Verizon wireless
	2600:1012:b166:2e5d:bde1:ae4:e479:dbc6	May 28 2019 04:01:26	Verizon wireless
	174.213.3.16	May 28 2019 03:28:41	Verizon wireless
	174.213.3.16	May 28 2019 03:10:59	Verizon wireless
	174.213.3.16	May 27 2019 23:55:59	Verizon wireless
	97.46.128.180	May 27 2019 23:41:13	Verizon wireless
	174.213.7.229	May 27 2019 23:14:10	Verizon wireless
	174.213.7.229	May 27 2019 23:10:58	Verizon wireless
	76.176.201.7	May 27 2019 22:46:51	Spectrum
	76.176.201.7	May 27 2019 22:10:57	Spectrum
	76.176.201.7	May 27 2019 20:47:19	Spectrum
	2600:1012:b15f:3a4:ac6d:b6a6:e2d7:59e9	May 27 2019 20:21:23	Verizon wireless
	174.213.23.221	May 27 2019 04:10:58	Verizon wireless
	174.213.23.221	May 27 2019 03:10:21	Verizon wireless
	2600:1012:b15f:3a4:c418:ff8a:f825:9d45	May 27 2019 02:59:50	Verizon wireless
	97.46.133.107	May 26 2019 23:56:21	Verizon wireless
	174.213.28.174	May 26 2019 23:10:58	Verizon wireless

And

<u>Email</u>	<u>IP</u>	<u>Date</u>	<u>Provider</u>
	2600:1012:b167:f61f:e891:9aca:ffee:e32a	June 28 2019 02:10:56	Verizon wireless
	52.34.110.242	June 27 2019 23:20:30	Amazon
	52.34.110.242	June 27 2019 23:20:26	Amazon
	76.176.201.7	June 27 2019 23:20:25	Spectrum
	76.176.201.7	June 27 2019 23:20:21	Spectrum
	76.176.201.7	June 27 2019 23:18:32	Spectrum
	76.176.201.7	June 27 2019 23:01:13	Spectrum
	97.33.193.78	June 27 2019 22:34:09	Verizon wireless
	174.213.5.13	June 27 2019 22:30:17	Verizon wireless
	161.30.16.142	June 27 2019 22:21:38	Verizon wireless
	161.30.16.142	June 27 2019 22:21:36	Verizon wireless
	161.30.16.142	June 27 2019 21:55:34	Verizon wireless
	174.219.139.155	June 27 2019 19:11:00	Verizon wireless
	2600:1014:b05c:b8e3:b572:a741:285b:e35f	June 27 2019 19:04:16	Verizon wireless
	52.203.65.30	June 27 2019 18:33:49	Amazon
	52.203.80.37	June 27 2019 18:33:42	Amazon
	2001:48f8:72:7e1:791c:a1d1:7233:c38	June 27 2019 18:33:02	Midco Midco.net
	2001:48f8:72:7e1:791c:a1d1:7233:c38	June 27 2019 18:32:55	Midco Midco.net
	52.203.80.37	June 27 2019 17:41:59	Amazon
	52.203.65.30	June 27 2019 17:41:51	Amazon
	52.34.110.242	June 27 2019 16:54:19	Amazon
	52.13.221.77	June 27 2019 16:54:19	Amazon
	2001:579:84a0:7:a960:a32a:e606:c163	June 27 2019 16:54:13	Cox Communication
	97.35.65.250	June 27 2019 01:43:05	Verizon wireless
	97.41.1.50	June 27 2019 01:39:39	Verizon wireless
	97.35.67.243	June 27 2019 01:33:27	Verizon wireless
	97.35.66.25	June 27 2019 01:26:00	Verizon wireless
	97.35.64.60	June 27 2019 01:20:52	Verizon wireless
	97.35.64.67	June 27 2019 01:14:34	Verizon wireless
	97.41.2.39	June 27 2019 01:11:11	Verizon wireless
	97.41.1.65	June 27 2019 01:00:55	Verizon wireless
	97.35.66.62	June 27 2019 00:56:08	Verizon wireless
	97.41.1.65	June 27 2019 00:48:31	Verizon wireless
	97.35.64.255	June 27 2019 00:40:05	Verizon wireless
	97.41.2.31	June 27 2019 00:36:24	Verizon wireless
	97.35.67.103	June 27 2019 00:26:01	Verizon wireless
	97.41.0.192	June 27 2019 00:20:53	Verizon wireless
	97.35.64.13	June 27 2019 00:16:13	Verizon wireless
	97.41.2.17	June 27 2019 00:14:09	Verizon wireless
	174.219.143.219	June 26 2019 23:46:00	Verizon wireless

In the same Internet Service provider lookup regarding the IP address 2001:48f8:72:7e1:791c:a1d1:7233:c38 on June 27<sup>th</sup> 2019, I observed that it resolves back to Midco.net identified further as Midcontinent Communications (Midco) with a possible subscriber geolocation of Sioux Falls, SD. I also know that it is possible that a user could be remotely accessing computers in those locations from anywhere in the

world via the internet and the IP Address logged would geolocate to that location even if the user was not physically in that location.

Based on the information listed above it appears likely that the AOL account of [REDACTED] was being operated by Thomas Denny Sanford during the time that Oath, Inc. discovered the image files depicting child pornography. It appears likely that on June 27<sup>th</sup> 2019 that same user was likely accessing the online account [REDACTED] through the IPs maintained by Midcontinent Communications (Midco) which is based out of Sioux Falls, SD and shows a possible geolocation of Sioux Falls, SD for the IP address.

**The affiant wishes to draw the court's attention to the following facts regarding inferences from the above-mentioned facts that are based upon my knowledge, training and experience:**

Based upon my training and experience, I know that individuals involved in acts of child sexual exploitation including the manufacture, possession and distribution of child pornography may use various mechanisms to communicate with other offenders, including communications through various email accounts. Your affiant is aware that individuals involved in criminal activity may mask their identity and use a false alias. Your affiant is further aware that individuals involved in acts of child sexual exploitation including child pornography may create electronic accounts including e-mail accounts with false aliases to further their ability to communicate with other offenders and/or victims.

Based upon my training and experience, I know that individuals who use the Internet for the manufacture, possession or distribution of child pornography will often times keep or store images of minors engaging in prohibited sexual acts. These individuals will sometimes use various e-mail accounts to store the images of minors engaging in prohibited sexual acts.

Based upon my training and experience, I know that electronic and/or written communication may exist within an e-mail account, Internet Service Provider, Cellular network provider or elsewhere, demonstrating the access to child pornography and/or child sexual exploitation.

Based on my training and experience, I know that Electronic Service Providers who offer web-based email accounts often times store and maintain user content within their computer systems and computer servers. This user content often times includes the entire contents of a user's email account including subscriber information, IP address logs, connection logs along with actual email messages and email content. This user content is typically stored within computer systems, computer servers and other forms of digital storage owned and/or maintained by the Electronic Service Provider.

Based upon my training and experience, I know that many email providers and Electronic Service Providers do not monitor the content of messages being exchanged by users. Therefore, individuals who are involved with the possession of child pornography will often times use email accounts to communicate with victims or exchange contraband and illicit material with other individuals.

Based upon the geolocation information that was associated with the IP address of, 2001:48f8:72:7e1:791c:a1d1:7233:c38 it appears that this IP address was being leased by a Midcontinent Communications customer on the date of the offense that was detailed in the CyberTip and email account described above.

I know that the only way to determine the identity of the subscriber that a particular IP address has been leased to by an ISP is by obtaining the subscriber information and customer records directly from the ISP itself.

I know that the Midcontinent Communications (Midco) keeps and maintains records and information about its customers/subscribers. This information includes customer records and logs regarding which IP address(es) were assigned to a Midcontinent Communications (Midco) subscriber for a particular date and time or a particular time period. Midcontinent Communications (Midco) requires the issuance of a subpoena or search warrant in order to provide subscriber information to law enforcement.

Your affiant knows that Midco.net or Midcontinent Communications is an internet service provider that is based out of Sioux Falls, SD. The vice president and General Counsel for Midco is identified with a physical address of 3901 N. Louise Ave. Sioux Falls SD 57107 and provides telephone, internet, and television service to several counties in South Dakota and also Minnesota, North Dakota, and Kansas

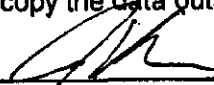
Based upon the information described above, I have probable cause to believe that on the computer systems owned, maintained, and/or operated by the company known as Midcontinent Communications (Midco) there exists evidence, fruits, and instrumentalities of violations of state and/or federal law. By this Affidavit and application, I respectfully request that the Court issue a search warrant directed to Midcontinent Communications (Midco) allowing agents to seize the records and subscriber information stored on the Midcontinent Communications (Midco) computer systems and computer servers for the IP address of 2001:48f8:72:7e1:791c:a1d1:7233:c38 .

For these reasons, I request authority to seize all customer records and subscriber information stored by the Midcontinent Communications (Midco) regarding the IP address listed above, to be searched off-site in a controlled environment. Law enforcement officers and agents will review the records sought by the search warrant and will segregate any records or information constituting evidence, fruits or instrumentalities of violations of state and/or federal criminal law. Additionally, I request authority to serve the warrant on Midstate Communications by electronic means and to allow the Midstate Communications to copy the data outside of this officer's presence.


Based upon my training and experience, I know that it is the policy of many providers to notify users about legal process that has been served in relation to the user's account. However, I also know that Oath Inc, Verizon wireless and Midcontinent Communications (Midco), will not notify user's about legal process where prohibited by law and/or court order. Therefore, I am requesting that Oath Inc, Verizon wireless and Midcontinent Communications (Midco) be prohibited from notifying any user or account holder of the existence of this legal process. I believed that if notification is given to the user it would likely result in the loss and/or destruction of evidence and would impede the ongoing investigative efforts of law enforcement.

Based upon the information described above, I have probable cause to believe that on the computer systems owned, maintained, and/or operated by the company known as Midcontinent Communications (Midco) in the United States, 3901 N Louise Avenue, Sioux Falls, SD 57107, there exists evidence, fruits, and instrumentalities of violations of state and/or federal law. By this Affidavit and application, I respectfully request that the Court issue a search warrant directed to Midcontinent Communications (Midco), allowing agents to seize the electronic communications and other information stored on Midcontinent Communications (Midco) computer systems and computer servers for the IP address: 2001:48f8:72:7e1:791c:a1d1:7233:c38 on June 27<sup>th</sup> 2019 at 18:33:02 hours UTC and 18:32:55 hours UTC and the associated files described above.

For these reasons, I request authority to seize all electronic communications and other content stored in the Target Account, to be searched off-site in a controlled environment. Law enforcement officers and agents will review the records sought by the search warrant and will segregate any messages and content constituting evidence, fruits or instrumentalities of violations of state and/or federal criminal law. Additionally, I request authority to serve the warrant on the Midcontinent Communications by facsimile and to allow Midcontinent Communication's to copy the data outside of this officer's presence.

  
\_\_\_\_\_  
Special Agent Jeff Kollars  
Division of Criminal Investigation

Subscribed and sworn to before me this 12<sup>th</sup> day of March, 2020.

  
\_\_\_\_\_  
(Notary Public)  
My commission expires 9/15/23

**FILED**  
MAY 08 2020  
Minnehaha County, S.D.  
Clerk Circuit Court

STATE OF SOUTH DAKOTA )  
 : SS  
COUNTY OF MINNEHAHA )

IN CIRCUIT COURT  
SECOND JUDICIAL CIRCUIT  
\*\*\*\*\*

STATE OF SOUTH DAKOTA,  
Plaintiff,

-vs-

AFFIDAVIT IN SUPPORT OF  
REQUEST FOR SEARCH  
WARRANT

THOMAS DENNY SANFORD  
DOB: [REDACTED]  
Defendant,

*SWA 90-403*

(In the matter of Possession and Distribution of Child Pornography in Minnehaha  
County, South Dakota)

\*\*\*\*\*  
The undersigned, being duly sworn upon oath, respectfully requests a Search Warrant to  
be issued for the following property:

ITEMS TO BE SEARCHED FOR AND SEIZED:

**Verizon Wireless Inc shall deliver to law enforcement the following records or  
information, in digital form (e.g. CD, DVD or by electronic document or file), dating  
from June 27<sup>th</sup> 2019 at 00:01 hours UTC to June 27<sup>th</sup> 2019 at 23:59 hours UTC:**

**Verizon Wireless Cellular Phone Number: [REDACTED]**

1. All business records and subscriber information, in any form kept,  
pertaining to the Verizon Wireless cellular number of [REDACTED]. Such  
information is to include but is not limited the following:
  - a. Full name of subscriber;
  - b. Address of subscriber;
  - c. All e-mail addresses listed on target account;
  - d. Other phone numbers associated with target account;
  - e. All available billing and payment information
  - f. Activation date of Target Account;
  - g. All available device information, to include make, model, serial  
number and IMEI number for all devices associated with Target  
Account.
2. Device Purchase Information. This is specifically to include the date, time  
and location of where the device or any pre-paid refill cards were  
purchased.
3. All available call detail records, including detailed information in reference  
to all known outgoing and incoming calls associated with the account,  
dates and times calls were made, and duration of all calls made or

received. This is to include any other pertinent call detail records including special features codes, or any other codes that are maintained in the normal course of business for Verizon Wireless. In addition to voice calls, this would also include any detail records showing text messages, MMS messages, or data activity.

4. All IP addresses assigned to or used by the Verizon Wireless cell phone number listed above.
5. Cell site information, to include all known cell towers associated with outgoing and incoming calls (Call Detail Records). This information is to include any sector information, if known, cell site location, and any other related material that would be necessary to identify the location and sector in reference to the cell site information associated with the call detail records. In the event text messages, MMS messages, LTE and Data activity including IP session and destination addresses that were produced are also available with cell site information, this information would be included in this request.
6. Cell site locations for all Verizon Wireless cell sites sector information including azimuth headings, in the regional market associated with the requested cell site information.
7. All historical device location information. This would include any reports of device activity that would include the approximate latitude and longitude of the device at the time of the activity, direction and distance from the tower, and other location related information commonly referred to as an RTT(Round Trip Timing), EVDO, ALULTE, and Levdot report. This further includes any other report similar in nature.

The information is being requested during the following time period

**Historical Records – June 27<sup>th</sup> 2019 at 00:01 hours UTC to June 27<sup>th</sup> 2019 at 23:59 hours UTC**

The undersigned respectfully requests that the Search Warrant be issued to permit a search at the following premises for the above-described property:


**The premises known as the offices of Verizon Wireless Inc Attn: VSAT in the United States located at 180 Washington Valley Road Bedminster, NJ 07921 and all computer systems and digital storage contained within, accessible from or associated regarding the following phone number [REDACTED]**




VERIZON WIRELESS INC (VSAT) IS PROHIBITED FROM NOTIFYING ANY USER OR ACCOUNT HOLDER OF THE EXISTANCE OF THE SEARCH WARRANT OR THAT THE SEARCH WARRANT HAD BEEN SERVED TO VERIZON WIRELESS. NOTIFICATION OF THE EXISTENCE OF THE SEARCH WARRANT TO THE USER OF THE ACCOUNT LISTED ABOVE WOULD LIKELY RESULT IN THE LOSS AND/OR DESTRUCTION OF EVIDENCE AND WOULD IMPEDE THE ONGOING INVESTIGATIVE EFFORTS OF LAW ENFORCEMENT.

(PLACE INITIALS IN THE APPROPRIATE BLANK)

 Property that constitutes evidence of the commission of a criminal offense;

 Contraband, the fruits of a crime, or things otherwise criminally possessed:

 Property designed or intended for use in, or which is or has been used as the means of committing a criminal offense

The undersigned further requests:

(PLACE INITIALS IN THE APPROPRIATE BLANK)

Execution of Search Warrant at night pursuant to SDCL 23A-35-4;

That no notice be given prior to the execution of the Search Warrant pursuant to SDCL 23A-35-9;

Authorization to serve the Search Warrant on Sunday;

 Execution of the Search Warrant during the daytime.

The facts in support of the issuance of a Search Warrant are as follows:

**Investigator Information:**

I, Jeff Kollars, am a Special Agent with the South Dakota Division of Criminal Investigation (DCI), Office of Attorney General for the State of South Dakota. As such, I am a state law enforcement officer responsible for the investigation of felony crimes committed in the State of South Dakota as required in SDCL 23-3-10. I am currently assigned to the Brookings, South Dakota DCI office and am responsible for conducting general criminal investigations in conjunction with, or independently from, local law enforcement. I have been assigned as a general crimes investigator for the DCI since May of 2013 and in that time have conducted investigations into all manner of criminal activity. This would include investigations into the offenses of rape, possession of child pornography, assault, theft, embezzlement, forgery, drug crimes, death investigations, and missing person cases.

I have been a sworn law enforcement officer in the State of South Dakota since May of 2006 and was employed as a State Trooper with the SD Highway Patrol from 2005 to 2013. I have received specialized training in interviewing and interrogation, crime scene processing, evidence collection, sexual assault investigation, electronic crimes and homicide investigation. I have conducted numerous investigations with individuals

suspected of committing all manner of crimes. I hold a bachelor's of science degree in Criminal Justice from the University of South Dakota in Vermillion, SD.

I am familiar with the facts and circumstances described herein and make this affidavit based upon personal knowledge derived from my participation in this investigation, conclusions I have reached based on my training and experience, and upon information I believe to be reliable from oral and written reports about this investigation and other investigations which I have received from state or local law enforcement officers from other law enforcement agencies.

**Current Investigation:**

On August 14<sup>th</sup> 2019, the National Center for Missing and Exploited Children (NCMEC) sent a cyber tip to the South Dakota Internet Crimes Against Children (ICAC) Task Force. The Cyber Tip had been submitted to NCMEC by Oath Inc, Inc. on July 9<sup>th</sup> 2019. The cyber tip was regarding an AOL/ Oath Inc user account that contained image files that were suspected of depicting child pornography and child erotica. On August 15<sup>th</sup> 2019 the cyber tip was assigned to me for investigation.

Based upon my training, knowledge and experience, I know that AOL was merged with Yahoo.com into what is now called Oath Inc. Oath Inc. is a Verizon Communications Company. Oath Inc provides a law enforcement contact address of 22000 AOL Way Dulles, VA 20166. AOL has a range of integrated products for members including communication tools, mobile apps and services and subscription packages. It provides dial up internet access, AOL mail, AOL instant messenger and AOL Desktop which is an internet suite integrating a web browser, media player and instant messenger.

Upon review of the information that was contained in the cyber tip, I learned that on July 9<sup>th</sup> 2019 AOL / Oath Inc. discovered 36 image files contained within a AOL user account that was suspected of depicting child pornography.

The information provided by Oath, Inc. in the cyber tip indicated that the name for the AOL account in question was Denny Sanford with a phone number of [REDACTED]. The reported email address was [REDACTED]. A username of VEJ6VUOXNEO4D3EFGW7IORXFDU-aol was listed for the account. There was also an alternate email address of [REDACTED] reported.

Next, I reviewed the images reported to me from Oath Inc in the cyber tip. The 36 images were three separate unique images, repeated several times. The first image was identified as 129055062\_image.63-1.jpeg being a juvenile female standing nude facing the camera. Her breasts and vagina were visible in the image. In the background was some green foliage and white drapes. Her right hand is on her right hip. The estimated age of the female is 12 to 15 years old.

The second image that was also repeated is identified as 129055094\_image.89-1.jpeg. It can be described as a nude juvenile female standing facing the camera. Her breasts and vagina are visible in the image. There is snow in the background and her hair is brown. The estimated age of the juvenile is 8 to 12 years old.

The third image is 129055159\_image.65-1.jpeg and is also repeated several times. The image can be described as a nude juvenile female standing, facing the camera. Her left

hand is near her mouth and right hand on her abdomen. In the image, her right breast is visible along with her vagina. There is green foliage visible in the background. The estimated age of the female is 10 to 15 years old.

On September 3<sup>rd</sup>, 2019, I received a subpoena from the Brookings County States Attorney requesting account registration information for the Verizon phone number [REDACTED]. I later received a report back from Verizon identifying the account being registered to Premier Bank Card LLC effective from 3/5/2013 to present with a contact name of Dana Anthony (address of [REDACTED]).

I made several attempts to contact Dana Anthony with Premier Bank and was able to have a phone conversation with her on November 20<sup>th</sup>, 2019. In the conversation, she first told me that no one at the bank had the number listed above. She then told me that the number was used by Denny Sanford. She also provided me with his personal assistant, Cobyann Berglund's contact information [REDACTED].

On November 20<sup>th</sup>, 2019, I received a phone call from Attorney Marty Jackley who informed me that he was representing Denny Sanford and Premiere Bank. He stated that he anticipates cooperating with law enforcement but requested that all further communication go through him.

I also received subpoenas from the Brookings County States Attorney for account registration information for [REDACTED] and [REDACTED] from Oath Inc. The subpoenas were served and information later provided by Oath identifying [REDACTED] as being registered to Denny Sanford and an associated email of [REDACTED] and phone number of [REDACTED] (verified). The account was listed as terminated and created on November 12, 1997.

The returned information from Oath Inc. provided account registration for [REDACTED] as being registered to Cobyann Berglund with phone numbers [REDACTED] and [REDACTED] being associated with the account. The account was created November 12<sup>th</sup> 1997 and was listed as active.

For clarification purposes, I also served a subpoena to Brookings Municipal Utilities (BMU) for the number [REDACTED] which was listed as being associated with BMU in the cyber tip from a search that they had completed. On November 29<sup>th</sup>, 2019, I was informed by representatives from BMU that they had no record of an account with that number at any point.

I also conducted a driver license search in South Dakota of Denny Sanford in which I found an active driver license of Thomas Denny Sanford DOB: [REDACTED] with an address of [REDACTED] and a mailing address of [REDACTED].

I also conducted a web search of the name Denny Sanford which provided multiple records identifying Thomas Denny Sanford as a South Dakota businessman and philanthropist who was the founder of First Premier Bank and the CEO of its holding company, United National Corporation. A public records search revealed that Thomas Denny Sanford also owns residences in Scottsdale, AZ, Sioux Falls, SD and La Jolla, CA.

On December 9<sup>th</sup> 2020, I produced an affidavit in support of a search warrant for Oath Inc records and content of the email address [REDACTED]. The search warrant was presented to the Honorable Judge James Power of the 2<sup>nd</sup> Circuit in Sioux Falls, SD who later signed the warrant. I later served the warrant on Oath Inc.

On January 10<sup>th</sup> 2020, I received the account records including emails from Oath Inc. for [REDACTED] pursuant to the warrant mentioned above. In review of the content I observed the following emails:

- 1) Email from [REDACTED] to [REDACTED]
  - a. Sent: May 28<sup>th</sup>, 2019 4:48:59 PM UTC
  - b. With the signature line saying "Sent from my Verizon Samsung Galaxy smartphone"
  - c. Including one picture attachment identified as file name 20190528\_092836.jpg
  - d. A description of this the image 20190528\_092836.jpg is described by myself as follows: The image is of a prepubescent female laying on her back, completely nude. Her vagina is visible on the left portion of the image with her legs spread. Her right breast is visible, and her face is on the right side of the image. There is a portion of blue material visible in the upper right portion of the photograph. There are several lines of deviation visible making the image appear to be a picture taken of another screen.
  
- 2) Email from [REDACTED] to [REDACTED]
  - a. Sent May 29<sup>th</sup>, 2019 1:39:09 PM UTC
  - b. With the signature line saying "Sent from my Verizon Samsung Galaxy smartphone"
  - c. Including one picture attachment identified as file name 20190528\_092836.jpg
  - d. The image appears to be the exact same image as identified above (#1).
  
- 3) Email from [REDACTED] to [REDACTED]
  - a. Sent June 27<sup>th</sup>, 2019 12:33:02 PM UTC
  - b. The subject line is "Emailing: 0\_270" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:  
0\_270  
Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.
  - c. Including one picture attachment identified as file name 0\_270.jpg.
  - d. A description of this the image 0\_270.jpg is described by myself as

follows: a juvenile female standing nude facing the camera. Her breasts and vagina are visible in the image. In the background was some green foliage and white drapes. Her right hand is on her right hip. The estimated age of the female is 12 to 15 years old. This image appears to be the same image described above as the first image within the MCMEC cyber tip.

- 4) Email from [REDACTED] to [REDACTED]
  - a. Sent June 27<sup>th</sup>, 2019 12:34:04 PM UTC.
  - b. The subject line is "Emailing: 0\_735" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:  
0\_735  
Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.
  - c. Including one picture attachment identified as file name 0\_735.jpg
  - d. A description of this the image 0\_735.jpg is described by myself as follows: a juvenile female standing nude facing the camera. She has blonde chest high straight hair which is down. Her right arm is crossing her chest and is resting on her left shoulder. Her left arm is resting on her right hip. Her vagina and both breasts are visible. The background of the photograph has a body of water and the ground around her is grassy. Her estimated age is 10 to 14 years of age.
- 5) Email from [REDACTED] to [REDACTED]
  - a. Sent June 27<sup>th</sup>, 2019 12:34:46 PM UTC.
  - b. The subject line is "Emailing: 0\_189" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:  
0\_189  
Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.
  - c. Including one picture attachment identified as file name 0\_189.jpg
  - d. A description of this the image 0\_189.jpg is described by myself as follows: It can be described as a nude juvenile female standing facing the camera. Her breasts and vagina are visible in the image. There is snow in the background and her hair is brown. The estimated age of the juvenile is 8 to 12 years old. This image is the second image described above within the MCMEC cyber tip.
- 6) Email from [REDACTED] to [REDACTED]
  - a. Sent June 27<sup>th</sup>, 2019 5:47:00 PM UTC.

- b. The subject line is "Emailing: 0\_588" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:  
0\_588  
Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.
  - c. Including one picture attachment identified as file name 0\_588.jpg
  - d. A description of the image 0\_588.jpg is that of a nude juvenile female standing, facing the camera. Her left hand is near her mouth and right hand on her abdomen. There is green foliage visible in the background. The estimated age of the female is 10 to 15 years old. The child's bare breasts and vagina are visible in the image. This image is the third image described above within the MCMEC cyber tip.
- 7) Email from [REDACTED] to [REDACTED]
- a. Sent June 27<sup>th</sup>, 2019 5:47:37 PM UTC
  - b. The subject line is "Emailing: 0\_270" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:  
0\_270  
Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.
  - c. Including one picture attachment identified as file name 0\_270.jpg.
  - d. A description of this the image 0\_270.jpg is the same as listed above in number "3" and appears to be the same image sent again.
- 8) Email from [REDACTED] to [REDACTED]
- a. Sent June 27<sup>th</sup>, 2019 6:34:28 PM UTC
  - b. The subject line is "Emailing: 0\_270" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:  
0\_270  
Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.
  - c. Including one picture attachment identified as file name 0\_270.jpg.
  - d. A description of this the image 0\_270.jpg is the same as listed above in number "3" and appears to be the same image sent again.

In several of the above listed emails and numerous others in the [REDACTED]

account there are several possible identifiers for the type of device that was used. In the message body of the above emails, "Sent from my Verizon Samsung Galaxy smartphone" is observed. I also know that Verizon will commonly maintain device information in their business records including the make, model and IMEI numbers.

Also in the first email detailed above the image, I know from my training and experience that the naming convention from above for the image 20190528\_092836.jpg possibly identifies a date and a time that the image was taken and is a common naming convention for Android devices.

Based on my training and experience and all the information relied upon in this investigation, I feel that the content of the image files described above fit the definition of child pornography as described in South Dakota Codified Law and fit well within definition and section SDCL 22-24A-3:

*a. Possessing, manufacturing, or distributing child pornography—Felonies—Assessment. A person is guilty of possessing, manufacturing, or distributing child pornography if the person:*

- (1) Creates any visual depiction of a minor engaging in a prohibited sexual act, or in the simulation of such an act;*
- (2) Causes or knowingly permits the creation of any visual depiction of a minor engaged in a prohibited sexual act, or in the simulation of such an act; or*
- (3) Knowingly possesses, distributes, or otherwise disseminates any visual depiction of a minor engaging in a prohibited sexual act, or in the simulation of such an act.*

*Consent to performing these proscribed acts by a minor or a minor's parent, guardian, or custodian, or mistake as to the minor's age is not a defense to a charge of violating this section.*

*A violation of this section is a Class 4 felony. If a person is convicted of a second or subsequent violation of this section within fifteen years of the prior conviction, the violation is a Class 3 felony.*

*The court shall order an assessment pursuant to § 22-22-1.3 of any person convicted of violating this section.*

*b. "Prohibited sexual act," actual or simulated sexual intercourse, sadism, masochism, sexual bestiality, incest, masturbation, or sadomasochistic abuse; actual or simulated exhibition of the genitals, the pubic or rectal area, or the bare feminine breasts, in a lewd or lascivious manner; actual physical contact with a person's clothed or unclothed genitals, pubic area, buttocks, or, if such person is a female, breast with the intent to arouse or gratify the sexual desire of either party; defecation or urination for the purpose of creating sexual excitement in the viewer; or any act or conduct which constitutes sexual battery or simulates that sexual battery is being or will be committed. The term includes encouraging, aiding, abetting or enticing any person to commit any such acts as provided in this subdivision. The term does not include a mother's breast-feeding of her baby;*

In review of the same emails included in the [REDACTED] account, several of the emails within the account include identifiers such as a photograph of a South Dakota Driver license of Thomas Denny Sanford DOB [REDACTED] with a physical address of [REDACTED] sent via email on 4/29/2019 via [REDACTED].

A letter from The Dalai Lama to T. Denny Sanford thanking him for support for a University of California San Diego T. Denny Sanford Institute for Empathy and Compassion dated 6/11/2019 sent from [REDACTED]

A photograph of a hotel receipt from the Curio Collection by Hilton of Coronado, California with a one night stay on February 9<sup>th</sup> 2019 and a guest name of Denny Sanford sent to email address [REDACTED] on February 6<sup>th</sup> 2019.

There were several photographs of a person that I believe to be Denny Sanford in a hospital gown, in an airplane, and sitting at a table. There were also photographs of decorative windows from Sanford Hospital in Sioux Falls, SD.

The same records received from Oath Inc for [REDACTED] included log in data with IP addresses from May 28<sup>th</sup> and 29<sup>th</sup> 2019 and also June 27<sup>th</sup> 2020.

I conducted Internet Service Provider (ISP) lookups regarding all of the IP addresses.

The IP addresses for May 28<sup>th</sup> and 29<sup>th</sup> 2019 and June 27<sup>th</sup>, 2019 and corresponding providers are as follows:



<u>Email address</u>	<u>IP</u>	<u>Date</u>	<u>Provider</u>
	174.213.18.4	May 30 2019 04:10:59	Verizon wireless
	52.34.110.242	May 29 2019 23:15:11	Amazon
	52.24.183.101	May 29 2019 23:13:03	Amazon
	54.190.199.109	May 29 2019 23:13:02	Amazon
	2001:579:84a0:7:e1b7:e997:dd64:50d1	May 29 2019 23:13:01	Cox Communication
	76.176.201.7	May 29 2019 23:10:59	Spectrum
	76.176.201.7	May 29 2019 23:01:18	Spectrum
	52.24.183.101	May 29 2019 22:54:52	Amazon
	52.34.110.242	May 29 2019 22:54:49	Amazon
	76.176.201.7	May 29 2019 22:54:47	Spectrum
	76.176.201.7	May 29 2019 22:54:44	Spectrum
	174.213.5.179	May 29 2019 21:11:00	Verizon wireless
	2600:1012:b15d:bb5f:9c37:a043:93db:30d0	May 29 2019 20:50:59	Verizon wireless
	174.213.5.179	May 29 2019 20:19:39	Verizon wireless
	174.212.21.98	May 29 2019 18:10:59	Verizon wireless
	34.221.128.86	May 29 2019 16:46:43	Amazon
	76.176.201.7	May 29 2019 15:18:15	Spectrum
	2600:1012:b100:bb44:6998:c8dd:f2e:96ae	May 29 2019 04:49:55	Verizon wireless
	174.212.9.9	May 29 2019 04:10:59	Verizon wireless
	2600:1012:b100:bb44:6998:c8dd:f2e:96ae	May 28 2019 23:24:52	Verizon wireless
	52.24.183.101	May 28 2019 23:11:53	Amazon
	54.191.16.110	May 28 2019 23:11:52	Amazon
	2001:579:84a0:7:3c42:625e:6757:442	May 28 2019 23:11:51	Cox Communication
	174.212.9.9	May 28 2019 23:11:00	Verizon wireless
	2600:1012:b16b:c79c:7c14:e651:2f51:286a	May 28 2019 22:14:48	Verizon wireless
	76.176.201.7	May 28 2019 21:24:43	Spectrum
	76.176.201.7	May 28 2019 21:12:13	Spectrum
	76.176.201.7	May 28 2019 21:10:59	Spectrum
	52.24.183.101	May 28 2019 18:45:46	Amazon
	52.34.110.242	May 28 2019 18:45:42	Amazon
	76.176.201.7	May 28 2019 18:45:41	Spectrum
	76.176.201.7	May 28 2019 18:45:37	Spectrum
	18.237.215.236	May 28 2019 17:54:02	Amazon
	76.176.201.7	May 28 2019 17:54:01	Spectrum
	76.176.201.7	May 28 2019 17:30:52	Spectrum
	52.34.110.242	May 28 2019 16:29:48	Amazon
	34.221.128.86	May 28 2019 16:25:08	Amazon
	174.213.9.175	May 28 2019 05:14:07	Verizon wireless
	174.213.9.175	May 28 2019 05:11:08	Verizon wireless
	2600:1012:b166:2e5d:bde1:aee4:e479:dbc6	May 28 2019 04:01:26	Verizon wireless
	174.213.3.16	May 28 2019 03:28:41	Verizon wireless
	174.213.3.16	May 28 2019 03:10:59	Verizon wireless
	174.213.3.16	May 27 2019 23:55:59	Verizon wireless
	97.46.128.180	May 27 2019 23:41:13	Verizon wireless
	174.213.7.229	May 27 2019 23:14:10	Verizon wireless
	174.213.7.229	May 27 2019 23:10:58	Verizon wireless
	76.176.201.7	May 27 2019 22:46:51	Spectrum
	76.176.201.7	May 27 2019 22:10:57	Spectrum
	76.176.201.7	May 27 2019 20:47:19	Spectrum
	2600:1012:b15f:3a4:ac6d:b6a6:e2d7:59e9	May 27 2019 20:21:23	Verizon wireless
	174.213.23.221	May 27 2019 04:10:58	Verizon wireless
	174.213.23.221	May 27 2019 03:10:21	Verizon wireless
	2600:1012:b15f:3a4:c418:ff8a:f825:9d45	May 27 2019 02:59:50	Verizon wireless
	97.46.133.107	May 26 2019 23:56:21	Verizon wireless
	174.213.28.174	May 26 2019 23:10:58	Verizon wireless

And

<u>Email</u>	<u>IP</u>	<u>Date</u>	<u>Provider</u>
	2600:1012:b167:f61f:e891:9aca:ffee:e32a	June 28 2019 02:10:56	Verizon wireless
	52.34.110.242	June 27 2019 23:20:30	Amazon
	52.34.110.242	June 27 2019 23:20:26	Amazon
	76.176.201.7	June 27 2019 23:20:25	Spectrum
	76.176.201.7	June 27 2019 23:20:21	Spectrum
	76.176.201.7	June 27 2019 23:18:32	Spectrum
	76.176.201.7	June 27 2019 23:01:13	Spectrum
	97.33.193.78	June 27 2019 22:34:09	Verizon wireless
	174.213.5.13	June 27 2019 22:30:17	Verizon wireless
	161.30.16.142	June 27 2019 22:21:38	Verizon wireless
	161.30.16.142	June 27 2019 22:21:36	Verizon wireless
	161.30.16.142	June 27 2019 21:55:34	Verizon wireless
	174.219.139.155	June 27 2019 19:11:00	Verizon wireless
	2600:1014:b05c:b8e3:b572:a741:285b:e35f	June 27 2019 19:04:16	Verizon wireless
	52.203.65.30	June 27 2019 18:33:49	Amazon
	52.203.80.37	June 27 2019 18:33:42	Amazon
	2001:48f8:72:7e1:791c:a1d1:7233:c38	June 27 2019 18:33:02	Midco Midco.net
	2001:48f8:72:7e1:791c:a1d1:7233:c38	June 27 2019 18:32:55	Midco Midco.net
	52.203.80.37	June 27 2019 17:41:59	Amazon
	52.203.65.30	June 27 2019 17:41:51	Amazon
	52.34.110.242	June 27 2019 16:54:19	Amazon
	52.13.221.77	June 27 2019 16:54:19	Amazon
	2001:579:84a0:7:a960:a32a:e606:c163	June 27 2019 16:54:13	Cox Communication
	97.35.65.250	June 27 2019 01:43:05	Verizon wireless
	97.41.1.50	June 27 2019 01:39:39	Verizon wireless
	97.35.67.243	June 27 2019 01:33:27	Verizon wireless
	97.35.66.25	June 27 2019 01:26:00	Verizon wireless
	97.35.64.60	June 27 2019 01:20:52	Verizon wireless
	97.35.64.67	June 27 2019 01:14:34	Verizon wireless
	97.41.2.39	June 27 2019 01:11:11	Verizon wireless
	97.41.1.65	June 27 2019 01:00:55	Verizon wireless
	97.35.66.62	June 27 2019 00:56:08	Verizon wireless
	97.41.1.65	June 27 2019 00:48:31	Verizon wireless
	97.35.64.255	June 27 2019 00:40:05	Verizon wireless
	97.41.2.31	June 27 2019 00:36:24	Verizon wireless
	97.35.67.103	June 27 2019 00:26:01	Verizon wireless
	97.41.0.192	June 27 2019 00:20:53	Verizon wireless
	97.35.64.13	June 27 2019 00:16:13	Verizon wireless
	97.41.2.17	June 27 2019 00:14:09	Verizon wireless
	174.219.143.219	June 26 2019 23:46:00	Verizon wireless

In the same Internet Service provider lookup regarding the IP address 2001:48f8:72:7e1:791c:a1d1:7233:c38 on June 27<sup>th</sup> 2019, I observed that it resolves back to Midco.net identified further as Midcontinent Communications (Midco) with a possible subscriber geolocation of Sioux Falls, SD.

In the same IP lookup, I observed numerous other IP addresses on May 28<sup>th</sup> and 29<sup>th</sup> and also June 27<sup>th</sup> 2019 resolving back to Verizon wireless. The commonality of IP addresses through May 28<sup>th</sup> and 29<sup>th</sup> and June 27<sup>th</sup> 2019 is Verizon wireless IPs.

Outside of the IP addresses from Verizon and Midcontinent were other IP addresses resolving to other states including Amazon (Oregon), Cox communication (Arizona) and Spectrum (California).

Two of the outgoing email messages containing child pornography had been sent from the [REDACTED] email address on May 28<sup>th</sup> and May 29<sup>th</sup> 2019 had a signature line that read "Sent from my Verizon Samsung Galaxy smartphone". Therefore, it is apparent that on May 28<sup>th</sup> and 29<sup>th</sup> 2019, the email account listed above had been accessed by multiple Verizon Wireless IP addresses and at least two of the outgoing email messages sent from that email account had been sent from a Verizon Wireless Samsung Galaxy cell phone. As described above, the cell phone number of [REDACTED] is a Verizon Wireless cell phone number and is currently being used by Denny Sanford. It should also be noted that in addition to the two outgoing emails containing child porn on May 28<sup>th</sup> and 29<sup>th</sup> 2019, there were 14 additional outgoing email messages that had the same "Verizon Samsung Galaxy Smartphone" signature line between those two dates. Many of the outgoing messages were in the same general time frame as the two outgoing messages containing the child porn.

However, it should be noted, that the Verizon Wireless IP addresses that were used to access the [REDACTED] email account on May 28<sup>th</sup> and 29<sup>th</sup> and June 27<sup>th</sup> 2019 have possible subscriber geolocations that include locations in several different states. Therefore, based upon the inconsistent possible subscriber geolocation information associated with the Verizon Wireless IP addresses that were used to access the email account listed above on May 28<sup>th</sup> and 29<sup>th</sup> June 27<sup>th</sup> 2019, I am unable to make an accurate determination regarding the location of the individual who was accessing and using the email account on that date.

It should also be noted, that the same list of IP addresses used by [REDACTED] as indicated by Oath, also listed numerous other IP addresses registered to several other Internet service providers including Spectrum (aka Charter Communications), Amazon and Cox Communications that had been used to access the email account listed above on June 27<sup>th</sup> 2019. Those various IP addresses have possible subscriber geolocations that include locations in Arizona, Oregon and California. Therefore, based upon the various different possible subscriber geolocations associated with the IP addresses used to access the email account listed above on May 28<sup>th</sup> and 29<sup>th</sup> and June 27<sup>th</sup> 2019 that resolve back to the various different Internet service providers listed above, I am unable to make an accurate determination regarding the location of the individual who was accessing and using the email account on that date.

Based upon publicly available information, I know that Denny Sanford owns homes in Sioux Falls, SD, Scottsdale, AZ and La Jolla, CA. The Possible subscriber geolocation information regarding the IP addresses that were used to access the [REDACTED] email account on June 27<sup>th</sup> 2019 include all three of those cities and states and on May 28<sup>th</sup> and 29<sup>th</sup> 2019 include Scottsdale, AZ and La Jolla, CA. I also know that it is possible that a user could be remotely accessing computers in those locations from anywhere in the world via the internet and the IP Address logged would geolocate to that location even if the user was not physically in that location.

I know that that Verizon wireless maintains records for long periods of time that would include details about the cellular device that is associated with a specific cell phone number, the IP addresses that were assigned to a specific cell phone number and the physical location of a cellular device on a specific date and time.

Therefore, based upon the inconsistent nature of the various IP addresses that had been used to access the [REDACTED] email account on May 28<sup>th</sup> and 29<sup>th</sup> and June 27<sup>th</sup> 2019 the most reliable way to positively identify the individual who was using in the email account on that date and the reliable way to accurately determine the location of that individual is by obtaining records and information from Verizon Wireless regarding the cell phone number of [REDACTED]. Specifically, subscriber information, device information, call detail records, IP address information and historical location information from Verizon Wireless can be necessary and essential in order to make those determinations.

**The affiant wishes to draw the court's attention to the following facts regarding inferences from the above mentioned facts that are based upon my knowledge, training and experience:**

I know that cellular telephone service providers (Carriers) such as Verizon Wireless store and/or keep a large amount of data and information regarding their cellular service subscribers. This data and information is stored on computer servers and computer systems belonging to or operated by Verizon Wireless. This data and information can include subscriber information, device information, call detail records, text message detail records, text message content, multimedia message detail records, multimedia message content, IP address information, cellular data usage records, device location information, Cell Site location information along with other data and information.

I know that subscriber information obtained from a Cellular Carrier can be used to determine ownership of a specific cellular telephone number as well as ownership of a specific cellular device.

I know that the call detail records, text message detail records, multimedia message detail records and data usage records obtained from a Cellular Carrier can be used to determine who a specific cell phone number or cellular device was being used by at a particular date or time.

I know that historical device location information and historical cell site location information can be used to try to determine the location of a cellular telephone or cellular device when a specific device activity such as a phone call, text message, multimedia message or email message took place. Also, this historical location information can be used to determine the location of a specific cellular user at a specific date and time in the past.

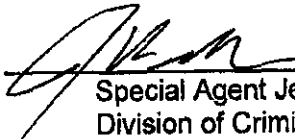
I know that the only way to determine the identity of the subscriber that a particular IP address has been leased to by an ISP or cellular provider is by obtaining the subscriber information and customer records directly from the ISP or cellular provider.

Based upon my training and experience, I know that it is the policy of many ISPs or cellular carriers to notify users about legal process that has been served in relation to the

user's account. However, I also know that Oath Inc, Verizon wireless, Midcontinent Communications (Midco), will not notify user's about legal process where prohibited by law and/or court order. Therefore, I am requesting that Oath Inc, Verizon wireless, Midcontinent Communications (Midco) be prohibited from notifying the users and specifically users of the email account with the email address of [REDACTED] or phone number of [REDACTED] of the existence of this legal process. I believed that if notification is given to the user it would likely result in the loss and/or destruction of evidence and would impede the ongoing investigative efforts of law enforcement.

Based upon the information described above, I have probable cause to believe that on the computer systems owned, maintained, and/or operated by the company known as Verizon Wireless there exists evidence, fruits, and instrumentalities of violations of state and/or federal law. By this Affidavit and application, I respectfully request that the Court issue a search warrant directed to Verizon Wireless, allowing agents to seize the electronic communications and other information stored on Verizon Wireless computer systems and computer servers for the phone number [REDACTED] and the associated files described above.

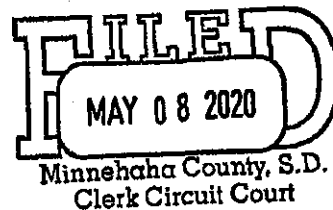
For these reasons, I request authority to seize all electronic communications and other content stored in the Target Account, to be searched off-site in a controlled environment. Law enforcement officers and agents will review the records sought by the search warrant and will segregate any messages and content constituting evidence, fruits or instrumentalities of violations of state and/or federal criminal law. Additionally, I request authority to serve the warrant on the Verizon Wireless by facsimile and to allow Verizon Wireless to copy the data outside of this officer's presence.

  
Special Agent Jeff Kollars  
Division of Criminal Investigation

Subscribed and sworn to before me this 12<sup>th</sup> day of March, 2020.

  
(Notary Public)

My commission expires 9/15/23



STATE OF SOUTH DAKOTA )  
 : SS  
COUNTY OF MINNEHAHA )  
\*\*\*\*\*

IN CIRCUIT COURT  
SECOND JUDICIAL CIRCUIT  
\*\*\*\*\*

STATE OF SOUTH DAKOTA,  
Plaintiff,  
-vs-

AFFIDAVIT IN SUPPORT OF  
REQUEST FOR SEARCH  
WARRANT

THOMAS DENNY SANFORD  
DOB: [REDACTED]  
Defendant,

*JWA 20-464*

(In the matter of Possession and Distribution of Child Pornography in Minnehaha  
County, South Dakota)

\*\*\*\*\*  
The undersigned, being duly sworn upon oath, respectfully requests a Search Warrant to  
be issued for the following property:

ITEMS TO BE SEARCHED FOR AND SEIZED:

**Verizon Wireless Inc shall deliver to law enforcement the following records or  
information, in digital form (e.g. CD, DVD or by electronic document or file), dating  
from May 29<sup>th</sup> 2019 at 00:01 hours UTC to May 29<sup>th</sup> 2019 at 23:59 hours UTC:**

**Verizon Wireless Cellular Phone Number: [REDACTED]**

1. All business records and subscriber information, in any form kept,  
pertaining to the Verizon Wireless cellular number of [REDACTED]. Such  
information is to include but is not limited the following:
  - a. Full name of subscriber;
  - b. Address of subscriber;
  - c. All e-mail addresses listed on target account;
  - d. Other phone numbers associated with target account;
  - e. All available billing and payment information
  - f. Activation date of Target Account;
  - g. All available device information, to include make, model, serial  
number and IMEI number for all devices associated with Target  
Account.
2. Device Purchase Information. This is specifically to include the date, time  
and location of where the device or any pre-paid refill cards were  
purchased.
3. All available call detail records, including detailed information in reference  
to all known outgoing and incoming calls associated with the account,  
dates and times calls were made, and duration of all calls made or

received. This is to include any other pertinent call detail records including special features codes, or any other codes that are maintained in the normal course of business for Verizon Wireless. In addition to voice calls, this would also include any detail records showing text messages, MMS messages, or data activity.

4. All IP addresses assigned to or used by the Verizon Wireless cell phone number listed above.
5. Cell site information, to include all known cell towers associated with outgoing and incoming calls (Call Detail Records). This information is to include any sector information, if known, cell site location, and any other related material that would be necessary to identify the location and sector in reference to the cell site information associated with the call detail records. In the event text messages, MMS messages, LTE and Data activity including IP session and destination addresses that were produced are also available with cell site information, this information would be included in this request.
6. Cell site locations for all Verizon Wireless cell sites sector information including azimuth headings, in the regional market associated with the requested cell site information
7. All historical device location information. This would include any reports of device activity that would include the approximate latitude and longitude of the device at the time of the activity, direction and distance from the tower, and other location related information commonly referred to as an RTT(Round Trip Timing), EVDO, ALULTE, and Levdot report. This further includes any other report similar in nature.

The information is being requested during the following time period

**Historical Records – May 29<sup>th</sup> 2019 at 00:01 hours UTC to May 29<sup>th</sup> 2019 at 23:59 hours UTC**

The undersigned respectfully requests that the Search Warrant be issued to permit a search at the following premises for the above-described property:

The premises known as the offices of Verizon Wireless Inc Attn: VSAT in the United States located at 180 Washington Valley Road Bedminster, NJ 07921 and all computer systems and digital storage contained within, accessible from or associated regarding the following phone number [REDACTED]

VERIZON WIRELESS INC (VSAT) IS PROHIBITED FROM NOTIFYING ANY USER OR ACCOUNT HOLDER OF THE EXISTANCE OF THE SEARCH WARRANT OR THAT THE SEARCH WARRANT HAD BEEN SERVED TO VERIZON WIRELESS. NOTIFICATION OF THE EXISTENCE OF THE SEARCH WARRANT TO THE USER OF THE ACCOUNT LISTED ABOVE WOULD LIKELY RESULT IN THE LOSS AND/OR DESTRUCTION OF EVIDENCE AND WOULD IMPEDE THE ONGOING INVESTIGATIVE EFFORTS OF LAW ENFORCEMENT.

(PLACE INITIALS IN THE APPROPRIATE BLANK)

Property that constitutes evidence of the commission of a criminal offense;

Contraband, the fruits of a crime, or things otherwise criminally possessed;

Property designed or intended for use in, or which is or has been used as the means of committing a criminal offense

The undersigned further requests:

(PLACE INITIALS IN THE APPROPRIATE BLANK)

Execution of Search Warrant at night pursuant to SDCL 23A-35-4;

That no notice be given prior to the execution of the Search Warrant pursuant to SDCL 23A-35-9;

Authorization to serve the Search Warrant on Sunday;

Execution of the Search Warrant during the daytime.

The facts in support of the issuance of a Search Warrant are as follows:

**Investigator Information:**

I, Jeff Kollars, am a Special Agent with the South Dakota Division of Criminal Investigation (DCI), Office of Attorney General for the State of South Dakota. As such, I am a state law enforcement officer responsible for the investigation of felony crimes committed in the State of South Dakota as required in SDCL 23-3-10. I am currently assigned to the Brookings, South Dakota DCI office and am responsible for conducting general criminal investigations in conjunction with, or independently from, local law enforcement. I have been assigned as a general crimes investigator for the DCI since May of 2013 and in that time have conducted investigations into all manner of criminal activity. This would include investigations into the offenses of rape, possession of child pornography, assault, theft, embezzlement, forgery, drug crimes, death investigations, and missing person cases.

I have been a sworn law enforcement officer in the State of South Dakota since May of 2006 and was employed as a State Trooper with the SD Highway Patrol from 2005 to 2013. I have received specialized training in interviewing and interrogation, crime scene processing, evidence collection, sexual assault investigation, electronic crimes and homicide investigation. I have conducted numerous investigations with individuals



suspected of committing all manner of crimes. I hold a bachelor's of science degree in Criminal Justice from the University of South Dakota in Vermillion, SD.

I am familiar with the facts and circumstances described herein and make this affidavit based upon personal knowledge derived from my participation in this investigation, conclusions I have reached based on my training and experience, and upon information I believe to be reliable from oral and written reports about this investigation and other investigations which I have received from state or local law enforcement officers from other law enforcement agencies.

**Current Investigation:**

On August 14<sup>th</sup> 2019, the National Center for Missing and Exploited Children (NCMEC) sent a cyber tip to the South Dakota Internet Crimes Against Children (ICAC) Task Force. The Cyber Tip had been submitted to NCMEC by Oath Inc, Inc. on July 9<sup>th</sup> 2019. The cyber tip was regarding an AOL/ Oath Inc user account that contained image files that were suspected of depicting child pornography and child erotica. On August 15<sup>th</sup> 2019 the cyber tip was assigned to me for investigation.

Based upon my training, knowledge and experience, I know that AOL was merged with Yahoo.com into what is now called Oath Inc. Oath Inc. is a Verizon Communications Company. Oath Inc provides a law enforcement contact address of 22000 AOL Way Dulles, VA 20166. AOL has a range of integrated products for members including communication tools, mobile apps and services and subscription packages. It provides dial up internet access, AOL mail, AOL instant messenger and AOL Desktop which is an internet suite integrating a web browser, media player and instant messenger.

Upon review of the information that was contained in the cyber tip, I learned that on July 9<sup>th</sup> 2019 AOL / Oath Inc. discovered 36 image files contained within a AOL user account that was suspected of depicting child pornography.

The information provided by Oath, Inc. in the cyber tip indicated that the name for the AOL account in question was Denny Sanford with a phone number of [REDACTED]. The reported email address was [REDACTED]. A username of VEJ6VUOXNEO4D3EFGW7IORXFDU-aol was listed for the account. There was also an alternate email address of [REDACTED] reported.

Next, I reviewed the images reported to me from Oath Inc in the cyber tip. The 36 images were three separate unique images, repeated several times. The first image was identified as 129055062\_image.63-1.jpeg being a juvenile female standing nude facing the camera. Her breasts and vagina were visible in the image. In the background was some green foliage and white drapes. Her right hand is on her right hip. The estimated age of the female is 12 to 15 years old.

The second image that was also repeated is identified as 129055094\_image.89-1.jpeg. It can be described as a nude juvenile female standing facing the camera. Her breasts and vagina are visible in the image. There is snow in the background and her hair is brown. The estimated age of the juvenile is 8 to 12 years old.

The third image is 129055159\_image.65-1.jpeg and is also repeated several times. The image can be described as a nude juvenile female standing, facing the camera. Her left

hand is near her mouth and right hand on her abdomen. In the image, her right breast is visible along with her vagina. There is green foliage visible in the background. The estimated age of the female is 10 to 15 years old.

On September 3<sup>rd</sup>, 2019, I received a subpoena from the Brookings County States Attorney requesting account registration information for the Verizon phone number [REDACTED]. I later received a report back from Verizon identifying the account being registered to Premier Bank Card LLC effective from 3/5/2013 to present with a contact name of Dana Anthony (address of [REDACTED]).

I made several attempts to contact Dana Anthony with Premier Bank and was able to have a phone conversation with her on November 20<sup>th</sup>, 2019. In the conversation, she first told me that no one at the bank had the number listed above. She then told me that the number was used by Denny Sanford. She also provided me with his personal assistant, Cobyann Berglund's contact information [REDACTED].

On November 20<sup>th</sup>, 2019, I received a phone call from Attorney Marty Jackley who informed me that he was representing Denny Sanford and Premiere Bank. He stated that he anticipates cooperating with law enforcement but requested that all further communication go through him.

I also received subpoenas from the Brookings County States Attorney for account registration information for [REDACTED] and [REDACTED] from Oath Inc. The subpoenas were served and information later provided by Oath identifying [REDACTED] as being registered to Denny Sanford and an associated email of [REDACTED] and phone number of [REDACTED] (verified). The account was listed as terminated and created on November 12, 1997.

The returned information from Oath Inc. provided account registration for [REDACTED] as being registered to Cobyann Berglund with phone numbers [REDACTED] and [REDACTED] being associated with the account. The account was created November 12<sup>th</sup> 1997 and was listed as active.

For clarification purposes, I also served a subpoena to Brookings Municipal Utilities (BMU) for the number [REDACTED] which was listed as being associated with BMU in the cyber tip from a search that they had completed. On November 29<sup>th</sup>, 2019, I was informed by representatives from BMU that they had no record of an account with that number at any point.

I also conducted a driver license search in South Dakota of Denny Sanford in which I found an active driver license of Thomas Denny Sanford DOB: [REDACTED] with an address of [REDACTED] and a mailing address of [REDACTED].

I also conducted a web search of the name Denny Sanford which provided multiple records identifying Thomas Denny Sanford as a South Dakota businessman and philanthropist who was the founder of First Premier Bank and the CEO of its holding company, United National Corporation. A public records search revealed that Thomas Denny Sanford also owns residences in Scottsdale, AZ, Sioux Falls, SD and La Jolla, CA.

On December 9<sup>th</sup> 2020, I produced an affidavit in support of a search warrant for Oath Inc records and content of the email address [REDACTED]. The search warrant was presented to the Honorable Judge James Power of the 2<sup>nd</sup> Circuit in Sioux Falls, SD who later signed the warrant. I later served the warrant on Oath Inc.

On January 10<sup>th</sup> 2020, I received the account records including emails from Oath Inc. for [REDACTED] pursuant to the warrant mentioned above. In review of the content I observed the following emails:

- 1) Email from [REDACTED] to [REDACTED]
  - a. Sent: May 28<sup>th</sup>, 2019 4:48:59 PM UTC
  - b. With the signature line saying "Sent from my Verizon Samsung Galaxy smartphone"
  - c. Including one picture attachment identified as file name 20190528\_092836.jpg
  - d. A description of this the image 20190528\_092836.jpg is described by myself as follows: The image is of a prepubescent female laying on her back, completely nude. Her vagina is visible on the left portion of the image with her legs spread. Her right breast is visible, and her face is on the right side of the image. There is a portion of blue material visible in the upper right portion of the photograph. There are several lines of deviation visible making the image appear to be a picture taken of another screen.
- 2) Email from [REDACTED] to [REDACTED]
  - a. Sent May 29<sup>th</sup>, 2019 1:39:09 PM UTC
  - b. With the signature line saying "Sent from my Verizon Samsung Galaxy smartphone"
  - c. Including one picture attachment identified as file name 20190528\_092836.jpg
  - d. The image appears to be the exact same image as identified above (#1).
- 3) Email from [REDACTED] to [REDACTED]
  - a. Sent June 27<sup>th</sup>, 2019 12:33:02 PM UTC
  - b. The subject line is "Emailing: 0\_270" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:  
0\_270  
Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.
  - c. Including one picture attachment identified as file name 0\_270.jpg.
  - d. A description of this the image 0\_270.jpg is described by myself as

follows: a juvenile female standing nude facing the camera. Her breasts and vagina are visible in the image. In the background was some green foliage and white drapes. Her right hand is on her right hip. The estimated age of the female is 12 to 15 years old. This image appears to be the same image described above as the first image within the MCMEC cyber tip.

- 4) Email from [REDACTED] to [REDACTED]
  - a. Sent June 27<sup>th</sup>, 2019 12:34:04 PM UTC.
  - b. The subject line is "Emailing: 0\_735" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:  
0\_735  
Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.
  - c. Including one picture attachment identified as file name 0\_735.jpg
  - d. A description of this the image 0\_735.jpg is described by myself as follows: a juvenile female standing nude facing the camera. She has blonde chest high straight hair which is down. Her right arm is crossing her chest and is resting on her left shoulder. Her left arm is resting on her right hip. Her vagina and both breasts are visible. The background of the photograph has a body of water and the ground around her is grassy. Her estimated age is 10 to 14 years of age.
- 5) Email from [REDACTED] to [REDACTED]
  - a. Sent June 27<sup>th</sup>, 2019 12:34:46 PM UTC.
  - b. The subject line is "Emailing: 0\_189" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:  
0\_189  
Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.
  - c. Including one picture attachment identified as file name 0\_189.jpg
  - d. A description of this the image 0\_189.jpg is described by myself as follows: It can be described as a nude juvenile female standing facing the camera. Her breasts and vagina are visible in the image. There is snow in the background and her hair is brown. The estimated age of the juvenile is 8 to 12 years old. This image is the second image described above within the MCMEC cyber tip.
- 6) Email from [REDACTED] to [REDACTED]
  - a. Sent June 27<sup>th</sup>, 2019 5:47:00 PM UTC.

- b. The subject line is "Emailing: 0\_588" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:  
0\_588  
Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.
  - c. Including one picture attachment identified as file name 0\_588.jpg
  - d. A description of the image 0\_588.jpg is that of a nude juvenile female standing, facing the camera. Her left hand is near her mouth and right hand on her abdomen. There is green foliage visible in the background. The estimated age of the female is 10 to 15 years old. The child's bare breasts and vagina are visible in the image. This image is the third image described above within the MCMEC cyber tip.
- 7) Email from [REDACTED] to [REDACTED]
- a. Sent June 27<sup>th</sup>, 2019 5:47:37 PM UTC
  - b. The subject line is "Emailing: 0\_270" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:  
0\_270  
Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.
  - c. Including one picture attachment identified as file name 0\_270.jpg.
  - d. A description of this the image 0\_270.jpg is the same as listed above in number "3" and appears to be the same image sent again.
- 8) Email from [REDACTED] to [REDACTED]
- a. Sent June 27<sup>th</sup>, 2019 6:34:28 PM UTC
  - b. The subject line is "Emailing: 0\_270" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:  
0\_270  
Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.
  - c. Including one picture attachment identified as file name 0\_270.jpg.
  - d. A description of this the image 0\_270.jpg is the same as listed above in number "3" and appears to be the same image sent again.

In several of the above listed emails and numerous others in the [REDACTED]

account there are several possible identifiers for the type of device that was used. In the message body of the above emails, "Sent from my Verizon Samsung Galaxy smartphone" is observed. I also know that Verizon will commonly maintain device information in their business records including the make, model and IMEI numbers.

Also in the first email detailed above the image, I know from my training and experience that the naming convention from above for the image 20190528\_092836.jpg possibly identifies a date and a time that the image was taken and is a common naming convention for Android devices.

Based on my training and experience and all the information relied upon in this investigation, I feel that the content of the image files described above fit the definition of child pornography as described in South Dakota Codified Law and fit well within definition and section SDCL 22-24A-3:

a. *Possessing, manufacturing, or distributing child pornography--Felonies--Assessment. A person is guilty of possessing, manufacturing, or distributing child pornography if the person:*

(1) *Creates any visual depiction of a minor engaging in a prohibited sexual act, or in the simulation of such an act;*

(2) *Causes or knowingly permits the creation of any visual depiction of a minor engaged in a prohibited sexual act, or in the simulation of such an act; or*

(3) *Knowingly possesses, distributes, or otherwise disseminates any visual depiction of a minor engaging in a prohibited sexual act, or in the simulation of such an act.*

*Consent to performing these proscribed acts by a minor or a minor's parent, guardian, or custodian, or mistake as to the minor's age is not a defense to a charge of violating this section.*

*A violation of this section is a Class 4 felony. If a person is convicted of a second or subsequent violation of this section within fifteen years of the prior conviction, the violation is a Class 3 felony.*

*The court shall order an assessment pursuant to § 22-22-1.3 of any person convicted of violating this section.*

b. *"Prohibited sexual act," actual or simulated sexual intercourse, sadism, masochism, sexual bestiality, incest, masturbation, or sadomasochistic abuse; actual or simulated exhibition of the genitals, the pubic or rectal area, or the bare feminine breasts, in a lewd or lascivious manner; actual physical contact with a person's clothed or unclothed genitals, pubic area, buttocks, or, if such person is a female, breast with the intent to arouse or gratify the sexual desire of either party; defecation or urination for the purpose of creating sexual excitement in the viewer; or any act or conduct which constitutes sexual battery or simulates that sexual battery is being or will be committed. The term includes encouraging, aiding, abetting or enticing any person to commit any such acts as provided in this subdivision. The term does not include a mother's breast-feeding of her baby;*

In review of the same emails included in the [REDACTED] account, several of the emails within the account include identifiers such as a photograph of a South Dakota Driver license of Thomas Denny Sanford DOB [REDACTED] with a physical address of [REDACTED] sent via email on 4/29/2019 via [REDACTED]

A letter from The Dalai Lama to T. Denny Sanford thanking him for support for a University of California San Diego T. Denny Sanford Institute for Empathy and Compassion dated 6/11/2019 sent from [REDACTED]

A photograph of a hotel receipt from the Curio Collection by Hilton of Coronado, California with a one night stay on February 9<sup>th</sup> 2019 and a guest name of Denny Sanford sent to email address [REDACTED] on February 6<sup>th</sup> 2019.

There were several photographs of a person that I believe to be Denny Sanford in a hospital gown, in an airplane, and sitting at a table. There were also photographs of decorative windows from Sanford Hospital in Sioux Falls, SD.

The same records received from Oath Inc for [REDACTED] included log in data with IP addresses from May 28<sup>th</sup> and 29<sup>th</sup> 2019 and also June 27<sup>th</sup> 2020.

I conducted Internet Service Provider (ISP) lookups regarding all of the IP addresses.

The IP addresses for May 28<sup>th</sup> and 29<sup>th</sup> 2019 and June 27<sup>th</sup>, 2019 and corresponding providers are as follows:

<u>Email address</u>	<u>IP</u>	<u>Date</u>	<u>Provider</u>
	174.213.18.4	May 30 2019 04:10:59	Verizon wireless
	52.34.110.242	May 29 2019 23:15:11	Amazon
	52.24.183.101	May 29 2019 23:13:03	Amazon
	54.190.199.109	May 29 2019 23:13:02	Amazon
	2001:579:84a0:7:e1b7:e997:dd64:50d1	May 29 2019 23:13:01	Cox Communication
	76.176.201.7	May 29 2019 23:10:59	Spectrum
	76.176.201.7	May 29 2019 23:01:18	Spectrum
	52.24.183.101	May 29 2019 22:54:52	Amazon
	52.34.110.242	May 29 2019 22:54:49	Amazon
	76.176.201.7	May 29 2019 22:54:47	Spectrum
	76.176.201.7	May 29 2019 22:54:44	Spectrum
	174.213.5.179	May 29 2019 21:11:00	Verizon wireless
	2600:1012:b15d:bb5f:9c37:a043:93db:30d0	May 29 2019 20:50:59	Verizon wireless
	174.213.5.179	May 29 2019 20:19:39	Verizon wireless
	174.212.21.98	May 29 2019 18:10:59	Verizon wireless
	34.221.128.86	May 29 2019 16:46:43	Amazon
	76.176.201.7	May 29 2019 15:18:15	Spectrum
	2600:1012:b100:bb44:6998:c8dd:f2e:96ae	May 29 2019 04:49:55	Verizon wireless
	174.212.9.9	May 29 2019 04:10:59	Verizon wireless
	2600:1012:b100:bb44:6998:c8dd:f2e:96ae	May 28 2019 23:24:52	Verizon wireless
	52.24.183.101	May 28 2019 23:11:53	Amazon
	54.191.16.110	May 28 2019 23:11:52	Amazon
	2001:579:84a0:7:3c42:625e:6757:442	May 28 2019 23:11:51	Cox Communication
	174.212.9.9	May 28 2019 23:11:00	Verizon wireless
	2600:1012:b16b:c79c:7c14:e651:2f51:286a	May 28 2019 22:14:48	Verizon wireless
	76.176.201.7	May 28 2019 21:24:43	Spectrum
	76.176.201.7	May 28 2019 21:12:13	Spectrum
	76.176.201.7	May 28 2019 21:10:59	Spectrum
	52.24.183.101	May 28 2019 18:45:46	Amazon
	52.34.110.242	May 28 2019 18:45:42	Amazon
	76.176.201.7	May 28 2019 18:45:41	Spectrum
	76.176.201.7	May 28 2019 18:45:37	Spectrum
	18.237.215.236	May 28 2019 17:54:02	Amazon
	76.176.201.7	May 28 2019 17:54:01	Spectrum
	76.176.201.7	May 28 2019 17:30:52	Spectrum
	52.34.110.242	May 28 2019 16:29:48	Amazon
	34.221.128.86	May 28 2019 16:25:08	Amazon
	174.213.9.175	May 28 2019 05:14:07	Verizon wireless
	174.213.9.175	May 28 2019 05:11:08	Verizon wireless
	2600:1012:b166:2e5d:bde1:ae4:e479:dbc6	May 28 2019 04:01:26	Verizon wireless
	174.213.3.16	May 28 2019 03:28:41	Verizon wireless
	174.213.3.16	May 28 2019 03:10:59	Verizon wireless
	174.213.3.16	May 27 2019 23:55:59	Verizon wireless
	97.46.128.180	May 27 2019 23:41:13	Verizon wireless
	174.213.7.229	May 27 2019 23:14:10	Verizon wireless
	174.213.7.229	May 27 2019 23:10:58	Verizon wireless
	76.176.201.7	May 27 2019 22:46:51	Spectrum
	76.176.201.7	May 27 2019 22:10:57	Spectrum
	76.176.201.7	May 27 2019 20:47:19	Spectrum
	2600:1012:b15f:3a4:ac6d:b6a6:e2d7:59e9	May 27 2019 20:21:23	Verizon wireless
	174.213.23.221	May 27 2019 04:10:58	Verizon wireless
	174.213.23.221	May 27 2019 03:10:21	Verizon wireless
	2600:1012:b15f:3a4:c418:ff8a:f825:9d45	May 27 2019 02:59:50	Verizon wireless
	97.46.133.107	May 26 2019 23:56:21	Verizon wireless
	174.213.28.174	May 26 2019 23:10:58	Verizon wireless



And

<u>Email</u>	<u>IP</u>	<u>Date</u>	<u>Provider</u>
[REDACTED]	2600:1012:b167:f61f:e891:9aca:ffee:e32a	June 28 2019 02:10:56	Verizon wireless
[REDACTED]	52.34.110.242	June 27 2019 23:20:30	Amazon
[REDACTED]	52.34.110.242	June 27 2019 23:20:26	Amazon
[REDACTED]	76.176.201.7	June 27 2019 23:20:25	Spectrum
[REDACTED]	76.176.201.7	June 27 2019 23:20:21	Spectrum
[REDACTED]	76.176.201.7	June 27 2019 23:18:32	Spectrum
[REDACTED]	76.176.201.7	June 27 2019 23:01:13	Spectrum
[REDACTED]	97.33.193.78	June 27 2019 22:34:09	Verizon wireless
[REDACTED]	174.213.5.13	June 27 2019 22:30:17	Verizon wireless
[REDACTED]	161.30.16.142	June 27 2019 22:21:38	Verizon wireless
[REDACTED]	161.30.16.142	June 27 2019 22:21:36	Verizon wireless
[REDACTED]	161.30.16.142	June 27 2019 21:55:34	Verizon wireless
[REDACTED]	174.219.139.155	June 27 2019 19:11:00	Verizon wireless
[REDACTED]	2600:1014:b05c:b8e3:b572:a741:285b:e35f	June 27 2019 19:04:16	Verizon wireless
[REDACTED]	52.203.65.30	June 27 2019 18:33:49	Amazon
[REDACTED]	52.203.80.37	June 27 2019 18:33:42	Amazon
[REDACTED]	2001:48f8:72:7e1:791c:a1d1:7233:c38	June 27 2019 18:33:02	Midco Midco.net
[REDACTED]	2001:48f8:72:7e1:791c:a1d1:7233:c38	June 27 2019 18:32:55	Midco Midco.net
[REDACTED]	52.203.80.37	June 27 2019 17:41:59	Amazon
[REDACTED]	52.203.65.30	June 27 2019 17:41:51	Amazon
[REDACTED]	52.34.110.242	June 27 2019 16:54:19	Amazon
[REDACTED]	52.13.221.77	June 27 2019 16:54:19	Amazon
[REDACTED]	2001:579:84a0:7:a960:a32a:e606:c163	June 27 2019 16:54:13	Cox Communication
[REDACTED]	97.35.65.250	June 27 2019 01:43:05	Verizon wireless
[REDACTED]	97.41.1.50	June 27 2019 01:39:39	Verizon wireless
[REDACTED]	97.35.67.243	June 27 2019 01:33:27	Verizon wireless
[REDACTED]	97.35.66.25	June 27 2019 01:26:00	Verizon wireless
[REDACTED]	97.35.64.60	June 27 2019 01:20:52	Verizon wireless
[REDACTED]	97.35.64.67	June 27 2019 01:14:34	Verizon wireless
[REDACTED]	97.41.2.39	June 27 2019 01:11:11	Verizon wireless
[REDACTED]	97.41.1.65	June 27 2019 01:00:55	Verizon wireless
[REDACTED]	97.35.66.62	June 27 2019 00:56:08	Verizon wireless
[REDACTED]	97.41.1.65	June 27 2019 00:48:31	Verizon wireless
[REDACTED]	97.35.64.255	June 27 2019 00:40:05	Verizon wireless
[REDACTED]	97.41.2.31	June 27 2019 00:36:24	Verizon wireless
[REDACTED]	97.35.67.103	June 27 2019 00:26:01	Verizon wireless
[REDACTED]	97.41.0.192	June 27 2019 00:20:53	Verizon wireless
[REDACTED]	97.35.64.13	June 27 2019 00:16:13	Verizon wireless
[REDACTED]	97.41.2.17	June 27 2019 00:14:09	Verizon wireless
[REDACTED]	174.219.143.219	June 26 2019 23:46:00	Verizon wireless

In the same Internet Service provider lookup regarding the IP address 2001:48f8:72:7e1:791c:a1d1:7233:c38 on June 27<sup>th</sup> 2019, I observed that it resolves back to Midco.net identified further as Midcontinent Communications (Midco) with a possible subscriber geolocation of Sioux Falls, SD.

In the same IP lookup, I observed numerous other IP addresses on May 28<sup>th</sup> and 29<sup>th</sup> and also June 27<sup>th</sup> 2019 resolving back to Verizon wireless. The commonality of IP addresses through May 28<sup>th</sup> and 29<sup>th</sup> and June 27<sup>th</sup> 2019 is Verizon wireless IPs.

Outside of the IP addresses from Verizon and Midcontinent were other IP addresses resolving to other states including Amazon (Oregon), Cox communication (Arizona) and Spectrum (California).

Two of the outgoing email messages containing child pornography had been sent from the [REDACTED] email address on May 28<sup>th</sup> and May 29<sup>th</sup> 2019 had a signature line that read "Sent from my Verizon Samsung Galaxy smartphone". Therefore, it is apparent that on May 28<sup>th</sup> and 29<sup>th</sup> 2019, the email account listed above had been accessed by multiple Verizon Wireless IP addresses and at least two of the outgoing email messages sent from that email account had been sent from a Verizon Wireless Samsung Galaxy cell phone. As described above, the cell phone number of [REDACTED] is a Verizon Wireless cell phone number and is currently being used by Denny Sanford. It should also be noted that in addition to the two outgoing emails containing child porn on May 28<sup>th</sup> and 29<sup>th</sup> 2019, there were 14 additional outgoing email messages that had the same "Verizon Samsung Galaxy Smartphone" signature line between those two dates. Many of the outgoing messages were in the same general time frame as the two outgoing messages containing the child porn.

However, it should be noted, that the Verizon Wireless IP addresses that were used to access the [REDACTED] email account on May 28<sup>th</sup> and 29<sup>th</sup> and June 27<sup>th</sup> 2019 have possible subscriber geolocations that include locations in several different states. Therefore, based upon the inconsistent possible subscriber geolocation information associated with the Verizon Wireless IP addresses that were used to access the email account listed above on May 28<sup>th</sup> and 29<sup>th</sup> June 27<sup>th</sup> 2019, I am unable to make an accurate determination regarding the location of the individual who was accessing and using the email account on that date.

It should also be noted, that the same list of IP addresses used by [REDACTED] as indicated by Oath, also listed numerous other IP addresses registered to several other Internet service providers including Spectrum (aka Charter Communications), Amazon and Cox Communications that had been used to access the email account listed above on June 27<sup>th</sup> 2019. Those various IP addresses have possible subscriber geolocations that include locations in Arizona, Oregon and California. Therefore, based upon the various different possible subscriber geolocations associated with the IP addresses used to access the email account listed above on May 28<sup>th</sup> and 29<sup>th</sup> and June 27<sup>th</sup> 2019 that resolve back to the various different Internet service providers listed above, I am unable to make an accurate determination regarding the location of the individual who was accessing and using the email account on that date.

Based upon publicly available information, I know that Denny Sanford owns homes in Sioux Falls, SD, Scottsdale, AZ and La Jolla, CA. The Possible subscriber geolocation information regarding the IP addresses that were used to access the [REDACTED] email account on June 27<sup>th</sup> 2019 include all three of those cities and states and on May 28<sup>th</sup> and 29<sup>th</sup> 2019 include Scottsdale, AZ and Lajolla, CA. I also know that it is possible that a user could be remotely accessing computers in those locations from anywhere in the world via the internet and the IP Address logged would geolocate to that location even if the user was not physically in that location.

I know that that Verizon wireless maintains records for long periods of time that would include details about the cellular device that is associated with a specific cell phone number, the IP addresses that were assigned to a specific cell phone number and the physical location of a cellular device on a specific date and time.

Therefore, based upon the inconsistent nature of the various IP addresses that had been used to access the [REDACTED] email account on May 28<sup>th</sup> and 29<sup>th</sup> and June 27<sup>th</sup> 2019 the most reliable way to positively identify the individual who was using in the email account on that date and the reliable way to accurately determine the location of that individual is by obtaining records and information from Verizon Wireless regarding the cell phone number of [REDACTED]. Specifically, subscriber information, device information, call detail records, IP address information and historical location information from Verizon Wireless can be necessary and essential in order to make those determinations.

**The affiant wishes to draw the court's attention to the following facts regarding inferences from the above mentioned facts that are based upon my knowledge, training and experience:**

I know that cellular telephone service providers (Carriers) such as Verizon Wireless store and/or keep a large amount of data and information regarding their cellular service subscribers. This data and information is stored on computer servers and computer systems belonging to or operated by Verizon Wireless. This data and information can include subscriber information, device information, call detail records, text message detail records, text message content, multimedia message detail records, multimedia message content, IP address information, cellular data usage records, device location information, Cell Site location information along with other data and information.

I know that subscriber information obtained from a Cellular Carrier can be used to determine ownership of a specific cellular telephone number as well as ownership of a specific cellular device.

I know that the call detail records, text message detail records, multimedia message detail records and data usage records obtained from a Cellular Carrier can be used to determine who a specific cell phone number or cellular device was being used by at a particular date or time.

I know that historical device location information and historical cell site location information can be used to try to determine the location of a cellular telephone or cellular device when a specific device activity such as a phone call, text message, multimedia message or email message took place. Also, this historical location information can be used to determine the location of a specific cellular user at a specific date and time in the past.


I know that the only way to determine the identity of the subscriber that a particular IP address has been leased to by an ISP or cellular provider is by obtaining the subscriber information and customer records directly from the ISP or cellular provider.

Based upon my training and experience, I know that it is the policy of many ISPs or cellular carriers to notify users about legal process that has been served in relation to the

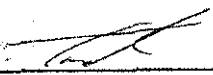
user's account. However, I also know that Oath Inc, Verizon wireless, Midcontinent Communications (Midco), will not notify user's about legal process where prohibited by law and/or court order. Therefore, I am requesting that Oath Inc, Verizon wireless, Midcontinent Communications (Midco) be prohibited from notifying the users and specifically users of the email account with the email address of [REDACTED] or phone number of [REDACTED] of the existence of this legal process. I believed that if notification is given to the user it would likely result in the loss and/or destruction of evidence and would impede the ongoing investigative efforts of law enforcement.

Based upon the information described above, I have probable cause to believe that on the computer systems owned, maintained, and/or operated by the company known as Verizon Wireless there exists evidence, fruits, and instrumentalities of violations of state and/or federal law. By this Affidavit and application, I respectfully request that the Court issue a search warrant directed to Verizon Wireless, allowing agents to seize the electronic communications and other information stored on Verizon Wireless computer systems and computer servers for the phone number [REDACTED] and the associated files described above.

For these reasons, I request authority to seize all electronic communications and other content stored in the Target Account, to be searched off-site in a controlled environment. Law enforcement officers and agents will review the records sought by the search warrant and will segregate any messages and content constituting evidence, fruits or instrumentalities of violations of state and/or federal criminal law. Additionally, I request authority to serve the warrant on the Verizon Wireless by facsimile and to allow Verizon Wireless to copy the data outside of this officer's presence.

  
Special Agent Jeff Kollars  
Division of Criminal Investigation

Subscribed and sworn to before me this 12 day of March, 2020.

  
\_\_\_\_\_  
(Notary Public)  
My commission expires 9/15/23

**FILED**  
MAY 08 2020  
Minnehaha County, S.D.  
Clerk Circuit Court



received. This is to include any other pertinent call detail records including special features codes, or any other codes that are maintained in the normal course of business for Verizon Wireless. In addition to voice calls, this would also include any detail records showing text messages, MMS messages, or data activity.

4. All IP addresses assigned to or used by the Verizon Wireless cell phone number listed above.
5. Cell site information, to include all known cell towers associated with outgoing and incoming calls (Call Detail Records). This information is to include any sector information, if known, cell site location, and any other related material that would be necessary to identify the location and sector in reference to the cell site information associated with the call detail records. In the event text messages, MMS messages, LTE and Data activity including IP session and destination addresses that were produced are also available with cell site information, this information would be included in this request.
6. Cell site locations for all Verizon Wireless cell sites sector information including azimuth headings, in the regional market associated with the requested cell site information
7. All historical device location information. This would include any reports of device activity that would include the approximate latitude and longitude of the device at the time of the activity, direction and distance from the tower, and other location related information commonly referred to as an RTT(Round Trip Timing), EVDO, ALULTE, and LevDort report. This further includes any other report similar in nature.

The information is being requested during the following time period

Historical Records – May 28<sup>th</sup> 2019 at 00:01 hours UTC to May 28<sup>th</sup> 2019 at 23:59 hours


UTC


The undersigned respectfully requests that the Search Warrant be issued to permit a search at the following premises for the above-described property:


The premises known as the offices of Verizon Wireless Inc Attn: VSAT in the United States located at 180 Washington Valley Road Bedminster, NJ 07921 and all computer systems and digital storage contained within, accessible from or associated regarding the following phone number [REDACTED]  
[REDACTED]

VERIZON WIRELESS INC (VSAT) IS PROHIBITED FROM NOTIFYING ANY USER OR ACCOUNT HOLDER OF THE EXISTANCE OF THE SEARCH WARRANT OR THAT THE SEARCH WARRANT HAD BEEN SERVED TO VERIZON WIRELESS. NOTIFICATION OF THE EXISTENCE OF THE SEARCH WARRANT TO THE USER OF THE ACCOUNT LISTED ABOVE WOULD LIKELY RESULT IN THE LOSS AND/OR DESTRUCTION OF EVIDENCE AND WOULD IMPEDE THE ONGOING INVESTIGATIVE EFFORTS OF LAW ENFORCEMENT.

(PLACE INITIALS IN THE APPROPRIATE BLANK)

 Property that constitutes evidence of the commission of a criminal offense;

 Contraband, the fruits of a crime, or things otherwise criminally possessed;

 Property designed or intended for use in, or which is or has been used as the means of committing a criminal offense

The undersigned further requests:

(PLACE INITIALS IN THE APPROPRIATE BLANK)

\_\_\_\_\_ Execution of Search Warrant at night pursuant to SDCL 23A-35-4;

\_\_\_\_\_ That no notice be given prior to the execution of the Search Warrant pursuant to SDCL 23A-35-9;

\_\_\_\_\_ Authorization to serve the Search Warrant on Sunday;

 Execution of the Search Warrant during the daytime.

The facts in support of the issuance of a Search Warrant are as follows:

**Investigator Information:**

I, Jeff Kollars, am a Special Agent with the South Dakota Division of Criminal Investigation (DCI), Office of Attorney General for the State of South Dakota. As such, I am a state law enforcement officer responsible for the investigation of felony crimes committed in the State of South Dakota as required in SDCL 23-3-10. I am currently assigned to the Brookings, South Dakota DCI office and am responsible for conducting general criminal investigations in conjunction with, or independently from, local law enforcement. I have been assigned as a general crimes investigator for the DCI since May of 2013 and in that time have conducted investigations into all manner of criminal activity. This would include investigations into the offenses of rape, possession of child pornography, assault, theft, embezzlement, forgery, drug crimes, death investigations, and missing person cases.

I have been a sworn law enforcement officer in the State of South Dakota since May of 2006 and was employed as a State Trooper with the SD Highway Patrol from 2005 to 2013. I have received specialized training in interviewing and interrogation, crime scene processing, evidence collection, sexual assault investigation, electronic crimes and homicide investigation. I have conducted numerous investigations with individuals

suspected of committing all manner of crimes. I hold a bachelor's of science degree in Criminal Justice from the University of South Dakota in Vermillion, SD.

I am familiar with the facts and circumstances described herein and make this affidavit based upon personal knowledge derived from my participation in this investigation, conclusions I have reached based on my training and experience, and upon information I believe to be reliable from oral and written reports about this investigation and other investigations which I have received from state or local law enforcement officers from other law enforcement agencies.

**Current Investigation:**

On August 14<sup>th</sup> 2019, the National Center for Missing and Exploited Children (NCMEC) sent a cyber tip to the South Dakota Internet Crimes Against Children (ICAC) Task Force. The Cyber Tip had been submitted to NCMEC by Oath Inc, Inc. on July 9<sup>th</sup> 2019. The cyber tip was regarding an AOL/ Oath Inc user account that contained image files that were suspected of depicting child pornography and child erotica. On August 15<sup>th</sup> 2019 the cyber tip was assigned to me for investigation.

Based upon my training, knowledge and experience, I know that AOL was merged with Yahoo.com into what is now called Oath Inc. Oath Inc. is a Verizon Communications Company. Oath Inc provides a law enforcement contact address of 22000 AOL Way Dulles, VA 20166. AOL has a range of integrated products for members including communication tools, mobile apps and services and subscription packages. It provides dial up internet access, AOL mail, AOL instant messenger and AOL Desktop which is an internet suite integrating a web browser, media player and instant messenger.

Upon review of the information that was contained in the cyber tip, I learned that on July 9<sup>th</sup> 2019 AOL / Oath Inc. discovered 36 image files contained within a AOL user account that was suspected of depicting child pornography.

The information provided by Oath, Inc. in the cyber tip indicated that the name for the AOL account in question was Denny Sanford with a phone number of [REDACTED]. The reported email address was [REDACTED]. A username of VEJ6VUOXNEO4D3EFGW7IORXFDU-aol was listed for the account. There was also an alternate email address of [REDACTED] reported.

Next, I reviewed the images reported to me from Oath Inc in the cyber tip. The 36 images were three separate unique images, repeated several times. The first image was identified as 129055062\_image.63-1.jpeg being a juvenile female standing nude facing the camera. Her breasts and vagina were visible in the image. In the background was some green foliage and white drapes. Her right hand is on her right hip. The estimated age of the female is 12 to 15 years old.

The second image that was also repeated is identified as 129055094\_image.89-1.jpeg. It can be described as a nude juvenile female standing facing the camera. Her breasts and vagina are visible in the image. There is snow in the background and her hair is brown. The estimated age of the juvenile is 8 to 12 years old.

The third image is 129055159\_image.65-1.jpeg and is also repeated several times. The image can be described as a nude juvenile female standing, facing the camera. Her left



hand is near her mouth and right hand on her abdomen. In the image, her right breast is visible along with her vagina. There is green foliage visible in the background. The estimated age of the female is 10 to 15 years old.

On September 3<sup>rd</sup>, 2019, I received a subpoena from the Brookings County States Attorney requesting account registration information for the Verizon phone number [REDACTED]. I later received a report back from Verizon identifying the account being registered to Premier Bank Card LLC effective from 3/5/2013 to present with a contact name of Dana Anthony (address of [REDACTED]).

I made several attempts to contact Dana Anthony with Premier Bank and was able to have a phone conversation with her on November 20<sup>th</sup>, 2019. In the conversation, she first told me that no one at the bank had the number listed above. She then told me that the number was used by Denny Sanford. She also provided me with his personal assistant, Cobyann Berglund's contact information [REDACTED].

On November 20<sup>th</sup>, 2019, I received a phone call from Attorney Marty Jackley who informed me that he was representing Denny Sanford and Premiere Bank. He stated that he anticipates cooperating with law enforcement but requested that all further communication go through him.

I also received subpoenas from the Brookings County States Attorney for account registration information for [REDACTED] and [REDACTED] from Oath Inc. The subpoenas were served and information later provided by Oath identifying [REDACTED] as being registered to Denny Sanford and an associated email of [REDACTED] and phone number of [REDACTED] (verified). The account was listed as terminated and created on November 12, 1997.

The returned information from Oath Inc. provided account registration for [REDACTED] as being registered to Cobyann Berglund with phone numbers [REDACTED] and [REDACTED] being associated with the account. The account was created November 12<sup>th</sup> 1997 and was listed as active.

For clarification purposes, I also served a subpoena to Brookings Municipal Utilities (BMU) for the number [REDACTED] which was listed as being associated with BMU in the cyber tip from a search that they had completed. On November 29<sup>th</sup>, 2019, I was informed by representatives from BMU that they had no record of an account with that number at any point.

I also conducted a driver license search in South Dakota of Denny Sanford in which I found an active driver license of Thomas Denny Sanford DOB: [REDACTED] with an address of [REDACTED] and a mailing address of [REDACTED].

I also conducted a web search of the name Denny Sanford which provided multiple records identifying Thomas Denny Sanford as a South Dakota businessman and philanthropist who was the founder of First Premier Bank and the CEO of its holding company, United National Corporation. A public records search revealed that Thomas Denny Sanford also owns residences in Scottsdale, AZ, Sioux Falls, SD and La Jolla, CA.

On December 9<sup>th</sup> 2020, I produced an affidavit in support of a search warrant for Oath Inc records and content of the email address [REDACTED]. The search warrant was presented to the Honorable Judge James Power of the 2<sup>nd</sup> Circuit in Sioux Falls, SD who later signed the warrant. I later served the warrant on Oath Inc.

On January 10<sup>th</sup> 2020, I received the account records including emails from Oath Inc. for [REDACTED] pursuant to the warrant mentioned above. In review of the content I observed the following emails:

- 1) Email from [REDACTED] to [REDACTED]
  - a. Sent: May 28<sup>th</sup>, 2019 4:48:59 PM UTC
  - b. With the signature line saying "Sent from my Verizon Samsung Galaxy smartphone"
  - c. Including one picture attachment identified as file name 20190528\_092836.jpg
  - d. A description of this the image 20190528\_092836.jpg is described by myself as follows: The image is of a prepubescent female laying on her back, completely nude. Her vagina is visible on the left portion of the image with her legs spread. Her right breast is visible, and her face is on the right side of the image. There is a portion of blue material visible in the upper right portion of the photograph. There are several lines of deviation visible making the image appear to be a picture taken of another screen.
- 2) Email from [REDACTED] to [REDACTED]
  - a. Sent May 29<sup>th</sup>, 2019 1:39:09 PM UTC
  - b. With the signature line saying "Sent from my Verizon Samsung Galaxy smartphone"
  - c. Including one picture attachment identified as file name 20190528\_092836.jpg
  - d. The image appears to be the exact same image as identified above (#1).
- 3) Email from [REDACTED] to [REDACTED]
  - a. Sent June 27<sup>th</sup>, 2019 12:33:02 PM UTC
  - b. The subject line is "Emailing: 0\_270" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:  
0\_270  
Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.
  - c. Including one picture attachment identified as file name 0\_270.jpg.
  - d. A description of this the image 0\_270.jpg is described by myself as

follows: a juvenile female standing nude facing the camera. Her breasts and vagina are visible in the image. In the background was some green foliage and white drapes. Her right hand is on her right hip. The estimated age of the female is 12 to 15 years old. This image appears to be the same image described above as the first image within the MCMEC cyber tip.

- 4) Email from [REDACTED] to [REDACTED]
  - a. Sent June 27<sup>th</sup>, 2019 12:34:04 PM UTC.
  - b. The subject line is "Emailing: 0\_735" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:  
0\_735  
Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.
  - c. Including one picture attachment identified as file name 0\_735.jpg
  - d. A description of this the image 0\_735.jpg is described by myself as follows: a juvenile female standing nude facing the camera. She has blonde chest high straight hair which is down. Her right arm is crossing her chest and is resting on her left shoulder. Her left arm is resting on her right hip. Her vagina and both breasts are visible. The background of the photograph has a body of water and the ground around her is grassy. Her estimated age is 10 to 14 years of age.
- 5) Email from [REDACTED] to [REDACTED]
  - a. Sent June 27<sup>th</sup>, 2019 12:34:46 PM UTC.
  - b. The subject line is "Emailing: 0\_189" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:  
0\_189  
Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.
  - c. Including one picture attachment identified as file name 0\_189.jpg
  - d. A description of this the image 0\_189.jpg is described by myself as follows: It can be described as a nude juvenile female standing facing the camera. Her breasts and vagina are visible in the image. There is snow in the background and her hair is brown. The estimated age of the juvenile is 8 to 12 years old. This image is the second image described above within the MCMEC cyber tip.
- 6) Email from [REDACTED] to [REDACTED]
  - a. Sent June 27<sup>th</sup>, 2019 5:47:00 PM UTC.

- b. The subject line is "Emailing: 0\_588" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:  
0\_588  
Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.
  - c. Including one picture attachment identified as file name 0\_588.jpg
  - d. A description of the image 0\_588.jpg is that of a nude juvenile female standing, facing the camera. Her left hand is near her mouth and right hand on her abdomen. There is green foliage visible in the background. The estimated age of the female is 10 to 15 years old. The child's bare breasts and vagina are visible in the image. This image is the third image described above within the MCMEC cyber tip.
- 7) Email from [REDACTED] to [REDACTED]
- a. Sent June 27<sup>th</sup>, 2019 5:47:37 PM UTC
  - b. The subject line is "Emailing: 0\_270" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:  
0\_270  
Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.
  - c. Including one picture attachment identified as file name 0\_270.jpg.
  - d. A description of this the image 0\_270.jpg is the same as listed above in number "3" and appears to be the same image sent again.
- 8) Email from [REDACTED] to [REDACTED]
- a. Sent June 27<sup>th</sup>, 2019 6:34:28 PM UTC
  - b. The subject line is "Emailing: 0\_270" with content of the email as follows:  
Your message is ready to be sent with the following file or link attachments:  
0\_270  
Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.
  - c. Including one picture attachment identified as file name 0\_270.jpg.
  - d. A description of this the image 0\_270.jpg is the same as listed above in number "3" and appears to be the same image sent again.

In several of the above listed emails and numerous others in the [REDACTED]

account there are several possible identifiers for the type of device that was used. In the message body of the above emails, "Sent from my Verizon Samsung Galaxy smartphone" is observed. I also know that Verizon will commonly maintain device information in their business records including the make, model and IMEI numbers.

Also in the first email detailed above the image, I know from my training and experience that the naming convention from above for the image 20190528\_092836.jpg possibly identifies a date and a time that the image was taken and is a common naming convention for Android devices.

Based on my training and experience and all the information relied upon in this investigation, I feel that the content of the image files described above fit the definition of child pornography as described in South Dakota Codified Law and fit well within definition and section SDCL 22-24A-3:

a. *Possessing, manufacturing, or distributing child pornography—Felonies—Assessment. A person is guilty of possessing, manufacturing, or distributing child pornography if the person:*

(1) *Creates any visual depiction of a minor engaging in a prohibited sexual act, or in the simulation of such an act;*

(2) *Causes or knowingly permits the creation of any visual depiction of a minor engaged in a prohibited sexual act, or in the simulation of such an act; or*

(3) *Knowingly possesses, distributes, or otherwise disseminates any visual depiction of a minor engaging in a prohibited sexual act, or in the simulation of such an act.*

*Consent to performing these proscribed acts by a minor or a minor's parent, guardian, or custodian, or mistake as to the minor's age is not a defense to a charge of violating this section.*

*A violation of this section is a Class 4 felony. If a person is convicted of a second or subsequent violation of this section within fifteen years of the prior conviction, the violation is a Class 3 felony.*

*The court shall order an assessment pursuant to § 22-22-1.3 of any person convicted of violating this section.*

b. *"Prohibited sexual act," actual or simulated sexual intercourse, sadism, masochism, sexual bestiality, incest, masturbation, or sadomasochistic abuse; actual or simulated exhibition of the genitals, the pubic or rectal area, or the bare feminine breasts, in a lewd or lascivious manner; actual physical contact with a person's clothed or unclothed genitals, pubic area, buttocks, or, if such person is a female, breast with the intent to arouse or gratify the sexual desire of either party; defecation or urination for the purpose of creating sexual excitement in the viewer; or any act or conduct which constitutes sexual battery or simulates that sexual battery is being or will be committed. The term includes encouraging, aiding, abetting or enticing any person to commit any such acts as provided in this subdivision. The term does not include a mother's breast-feeding of her baby;*

In review of the same emails included in the [REDACTED] account, several of the emails within the account include identifiers such as a photograph of a South Dakota Driver license of Thomas Denny Sanford DOB [REDACTED] with a physical address of [REDACTED] sent via email on 4/29/2019 via [REDACTED]

A letter from The Dalai Lama to T. Denny Sanford thanking him for support for a University of California San Diego T. Denny Sanford Institute for Empathy and Compassion dated 6/11/2019 sent from [REDACTED]

A photograph of a hotel receipt from the Curio Collection by Hilton of Coronado, California with a one night stay on February 9<sup>th</sup> 2019 and a guest name of Denny Sanford sent to email address [REDACTED] on February 6<sup>th</sup> 2019.

There were several photographs of a person that I believe to be Denny Sanford in a hospital gown, in an airplane, and sitting at a table. There were also photographs of decorative windows from Sanford Hospital in Sioux Falls, SD.

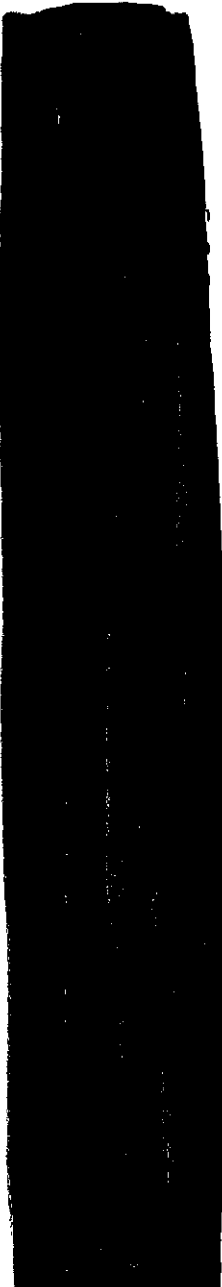
The same records received from Oath Inc for [REDACTED] included log in data with IP addresses from May 28<sup>th</sup> and 29<sup>th</sup> 2019 and also June 27<sup>th</sup> 2020.

I conducted Internet Service Provider (ISP) lookups regarding all of the IP addresses.

The IP addresses for May 28<sup>th</sup> and 29<sup>th</sup> 2019 and June 27<sup>th</sup>, 2019 and corresponding providers are as follows:

<u>Email address</u>	<u>IP</u>	<u>Date</u>	<u>Provider</u>
	174.213.18.4	May 30 2019 04:10:59	Verizon wireless
	52.34.110.242	May 29 2019 23:15:11	Amazon
	52.24.183.101	May 29 2019 23:13:03	Amazon
	54.190.199.109	May 29 2019 23:13:02	Amazon
	2001:579:84a0:7:e1b7:e997:dd64:50d1	May 29 2019 23:13:01	Cox Communication
	76.176.201.7	May 29 2019 23:10:59	Spectrum
	76.176.201.7	May 29 2019 23:01:18	Spectrum
	52.24.183.101	May 29 2019 22:54:52	Amazon
	52.34.110.242	May 29 2019 22:54:49	Amazon
	76.176.201.7	May 29 2019 22:54:47	Spectrum
	76.176.201.7	May 29 2019 22:54:44	Spectrum
	174.213.5.179	May 29 2019 21:11:00	Verizon wireless
	2600:1012:b15d:bb5f:9c37:a043:93db:30d0	May 29 2019 20:50:59	Verizon wireless
	174.213.5.179	May 29 2019 20:19:39	Verizon wireless
	174.212.21.98	May 29 2019 18:10:59	Verizon wireless
	34.221.128.86	May 29 2019 16:46:43	Amazon
	76.176.201.7	May 29 2019 15:18:15	Spectrum
	2600:1012:b100:bb44:6998:c8dd:f2e:96ae	May 29 2019 04:49:55	Verizon wireless
	174.212.9.9	May 29 2019 04:10:59	Verizon wireless
	2600:1012:b100:bb44:6998:c8dd:f2e:96ae	May 28 2019 23:24:52	Verizon wireless
	52.24.183.101	May 28 2019 23:11:53	Amazon
	54.191.16.110	May 28 2019 23:11:52	Amazon
	2001:579:84a0:7:3c42:625e:6757:442	May 28 2019 23:11:51	Cox Communication
	174.212.9.9	May 28 2019 23:11:00	Verizon wireless
	2600:1012:b16b:c79c:7c14:e651:2f51:286a	May 28 2019 22:14:48	Verizon wireless
	76.176.201.7	May 28 2019 21:24:43	Spectrum
	76.176.201.7	May 28 2019 21:12:13	Spectrum
	76.176.201.7	May 28 2019 21:10:59	Spectrum
	52.24.183.101	May 28 2019 18:45:46	Amazon
	52.34.110.242	May 28 2019 18:45:42	Amazon
	76.176.201.7	May 28 2019 18:45:41	Spectrum
	76.176.201.7	May 28 2019 18:45:37	Spectrum
	18.237.215.236	May 28 2019 17:54:02	Amazon
	76.176.201.7	May 28 2019 17:54:01	Spectrum
	76.176.201.7	May 28 2019 17:30:52	Spectrum
	52.34.110.242	May 28 2019 16:29:48	Amazon
	34.221.128.86	May 28 2019 16:25:08	Amazon
	174.213.9.175	May 28 2019 05:14:07	Verizon wireless
	174.213.9.175	May 28 2019 05:11:08	Verizon wireless
	2600:1012:b166:2e5d:bde1:ae4:e479:dbc6	May 28 2019 04:01:26	Verizon wireless
	174.213.3.16	May 28 2019 03:28:41	Verizon wireless
	174.213.3.16	May 28 2019 03:10:59	Verizon wireless
	174.213.3.16	May 27 2019 23:55:59	Verizon wireless
	97.46.128.180	May 27 2019 23:41:13	Verizon wireless
	174.213.7.229	May 27 2019 23:14:10	Verizon wireless
	174.213.7.229	May 27 2019 23:10:58	Verizon wireless
	76.176.201.7	May 27 2019 22:46:51	Spectrum
	76.176.201.7	May 27 2019 22:10:57	Spectrum
	76.176.201.7	May 27 2019 20:47:19	Spectrum
	2600:1012:b15f:3a4:ac6d:b6a6:e2d7:59e9	May 27 2019 20:21:23	Verizon wireless
	174.213.23.221	May 27 2019 04:10:58	Verizon wireless
	174.213.23.221	May 27 2019 03:10:21	Verizon wireless
	2600:1012:b15f:3a4:c418:ff8a:f825:9d45	May 27 2019 02:59:50	Verizon wireless
	97.46.133.107	May 26 2019 23:56:21	Verizon wireless
	174.213.28.174	May 26 2019 23:10:58	Verizon wireless

And

<u>Email</u>	<u>IP</u>	<u>Date</u>	<u>Provider</u>
	2600:1012:b167:f61f:e891:9aca:ffee:e32a	June 28 2019 02:10:56	Verizon wireless
	52.34.110.242	June 27 2019 23:20:30	Amazon
	52.34.110.242	June 27 2019 23:20:26	Amazon
	76.176.201.7	June 27 2019 23:20:25	Spectrum
	76.176.201.7	June 27 2019 23:20:21	Spectrum
	76.176.201.7	June 27 2019 23:18:32	Spectrum
	76.176.201.7	June 27 2019 23:01:13	Spectrum
	97.33.193.78	June 27 2019 22:34:09	Verizon wireless
	174.213.5.13	June 27 2019 22:30:17	Verizon wireless
	161.30.16.142	June 27 2019 22:21:38	Verizon wireless
	161.30.16.142	June 27 2019 22:21:36	Verizon wireless
	161.30.16.142	June 27 2019 21:55:34	Verizon wireless
	174.219.139.155	June 27 2019 19:11:00	Verizon wireless
	2600:1014:b05c:b8e3:b572:a741:285b:e35f	June 27 2019 19:04:16	Verizon wireless
	52.203.65.30	June 27 2019 18:33:49	Amazon
	52.203.80.37	June 27 2019 18:33:42	Amazon
	2001:48f8:72:7e1:791c:a1d1:7233:c38	June 27 2019 18:33:02	Midco Midco.net
	2001:48f8:72:7e1:791c:a1d1:7233:c38	June 27 2019 18:32:55	Midco Midco.net
	52.203.80.37	June 27 2019 17:41:59	Amazon
	52.203.65.30	June 27 2019 17:41:51	Amazon
	52.34.110.242	June 27 2019 16:54:19	Amazon
	52.13.221.77	June 27 2019 16:54:19	Amazon
	2001:579:84a0:7:a960:a32a:e606:c163	June 27 2019 16:54:13	Cox Communication
	97.35.65.250	June 27 2019 01:43:05	Verizon wireless
	97.41.1.50	June 27 2019 01:39:39	Verizon wireless
	97.35.67.243	June 27 2019 01:33:27	Verizon wireless
	97.35.66.25	June 27 2019 01:26:00	Verizon wireless
	97.35.64.60	June 27 2019 01:20:52	Verizon wireless
	97.35.64.67	June 27 2019 01:14:34	Verizon wireless
	97.41.2.39	June 27 2019 01:11:11	Verizon wireless
	97.41.1.65	June 27 2019 01:00:55	Verizon wireless
	97.35.66.62	June 27 2019 00:56:08	Verizon wireless
	97.41.1.65	June 27 2019 00:48:31	Verizon wireless
	97.35.64.255	June 27 2019 00:40:05	Verizon wireless
	97.41.2.31	June 27 2019 00:36:24	Verizon wireless
	97.35.67.103	June 27 2019 00:26:01	Verizon wireless
	97.41.0.192	June 27 2019 00:20:53	Verizon wireless
	97.35.64.13	June 27 2019 00:16:13	Verizon wireless
	97.41.2.17	June 27 2019 00:14:09	Verizon wireless
	174.219.143.219	June 26 2019 23:46:00	Verizon wireless

In the same Internet Service provider lookup regarding the IP address 2001:48f8:72:7e1:791c:a1d1:7233:c38 on June 27<sup>th</sup> 2019, I observed that it resolves back to Midco.net identified further as Midcontinent Communications (Midco) with a possible subscriber geolocation of Sioux Falls, SD.



In the same IP lookup, I observed numerous other IP addresses on May 28<sup>th</sup> and 29<sup>th</sup> and also June 27<sup>th</sup> 2019 resolving back to Verizon wireless. The commonality of IP addresses through May 28<sup>th</sup> and 29<sup>th</sup> and June 27<sup>th</sup> 2019 is Verizon wireless IPs.

Outside of the IP addresses from Verizon and Midcontinent were other IP addresses resolving to other states including Amazon (Oregon), Cox communication (Arizona) and Spectrum (California).

Two of the outgoing email messages containing child pornography had been sent from the [REDACTED] email address on May 28<sup>th</sup> and May 29<sup>th</sup> 2019 had a signature line that read "Sent from my Verizon Samsung Galaxy smartphone". Therefore, it is apparent that on May 28<sup>th</sup> and 29<sup>th</sup> 2019, the email account listed above had been accessed by multiple Verizon Wireless IP addresses and at least two of the outgoing email messages sent from that email account had been sent from a Verizon Wireless Samsung Galaxy cell phone. As described above, the cell phone number of [REDACTED] is a Verizon Wireless cell phone number and is currently being used by Denny Sanford. It should also be noted that in addition to the two outgoing emails containing child porn on May 28<sup>th</sup> and 29<sup>th</sup> 2019, there were 14 additional outgoing email messages that had the same "Verizon Samsung Galaxy Smartphone" signature line between those two dates. Many of the outgoing messages were in the same general time frame as the two outgoing messages containing the child porn.

However, it should be noted, that the Verizon Wireless IP addresses that were used to access the [REDACTED] email account on May 28<sup>th</sup> and 29<sup>th</sup> and June 27<sup>th</sup> 2019 have possible subscriber geolocations that include locations in several different states. Therefore, based upon the inconsistent possible subscriber geolocation information associated with the Verizon Wireless IP addresses that were used to access the email account listed above on May 28<sup>th</sup> and 29<sup>th</sup> June 27<sup>th</sup> 2019, I am unable to make an accurate determination regarding the location of the individual who was accessing and using the email account on that date.

It should also be noted, that the same list of IP addresses used by [REDACTED] as indicated by Oath, also listed numerous other IP addresses registered to several other Internet service providers including Spectrum (aka Charter Communications), Amazon and Cox Communications that had been used to access the email account listed above on June 27<sup>th</sup> 2019. Those various IP addresses have possible subscriber geolocations that include locations in Arizona, Oregon and California. Therefore, based upon the various different possible subscriber geolocations associated with the IP addresses used to access the email account listed above on May 28<sup>th</sup> and 29<sup>th</sup> and June 27<sup>th</sup> 2019 that resolve back to the various different Internet service providers listed above, I am unable to make an accurate determination regarding the location of the individual who was accessing and using the email account on that date.

Based upon publicly available information, I know that Denny Sanford owns homes in Sioux Falls, SD, Scottsdale, AZ and La Jolla, CA. The Possible subscriber geolocation information regarding the IP addresses that were used to access the [REDACTED] email account on June 27<sup>th</sup> 2019 include all three of those cities and states and on May 28<sup>th</sup> and 29<sup>th</sup> 2019 include Scottsdale, AZ and Lajolla, CA. I also know that it is possible that a user could be remotely accessing computers in those locations from anywhere in the world via the internet and the IP Address logged would geolocate to that location even if the user was not physically in that location.

I know that that Verizon wireless maintains records for long periods of time that would include details about the cellular device that is associated with a specific cell phone number, the IP addresses that were assigned to a specific cell phone number and the physical location of a cellular device on a specific date and time.

Therefore, based upon the inconsistent nature of the various IP addresses that had been used to access the [REDACTED] email account on May 28<sup>th</sup> and 29<sup>th</sup> and June 27<sup>th</sup> 2019 the most reliable way to positively identify the individual who was using in the email account on that date and the reliable way to accurately determine the location of that individual is by obtaining records and information from Verizon Wireless regarding the cell phone number of [REDACTED]. Specifically, subscriber information, device information, call detail records, IP address information and historical location information from Verizon Wireless can be necessary and essential in order to make those determinations.

**The affiant wishes to draw the court's attention to the following facts regarding inferences from the above mentioned facts that are based upon my knowledge, training and experience:**

I know that cellular telephone service providers (Carriers) such as Verizon Wireless store and/or keep a large amount of data and information regarding their cellular service subscribers. This data and information is stored on computer servers and computer systems belonging to or operated by Verizon Wireless. This data and information can include subscriber information, device information, call detail records, text message detail records, text message content, multimedia message detail records, multimedia message content, IP address information, cellular data usage records, device location information, Cell Site location information along with other data and information.

I know that subscriber information obtained from a Cellular Carrier can be used to determine ownership of a specific cellular telephone number as well as ownership of a specific cellular device.

I know that the call detail records, text message detail records, multimedia message detail records and data usage records obtained from a Cellular Carrier can be used to determine who a specific cell phone number or cellular device was being used by at a particular date or time.

I know that historical device location information and historical cell site location information can be used to try to determine the location of a cellular telephone or cellular device when a specific device activity such as a phone call, text message, multimedia message or email message took place. Also, this historical location information can be used to determine the location of a specific cellular user at a specific date and time in the past.

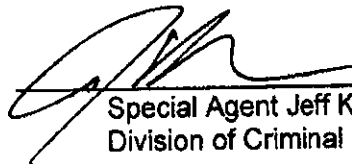
I know that the only way to determine the identity of the subscriber that a particular IP address has been leased to by an ISP or cellular provider is by obtaining the subscriber information and customer records directly from the ISP or cellular provider.

Based upon my training and experience, I know that it is the policy of many ISPs or cellular carriers to notify users about legal process that has been served in relation to the

user's account. However, I also know that Oath Inc, Verizon wireless, Midcontinent Communications (Midco), will not notify user's about legal process where prohibited by law and/or court order. Therefore, I am requesting that Oath Inc, Verizon wireless, Midcontinent Communications (Midco) be prohibited from notifying the users and specifically users of the email account with the email address of [REDACTED] or phone number of [REDACTED] of the existence of this legal process. I believed that if notification is given to the user it would likely result in the loss and/or destruction of evidence and would impede the ongoing investigative efforts of law enforcement.

Based upon the information described above, I have probable cause to believe that on the computer systems owned, maintained, and/or operated by the company known as Verizon Wireless there exists evidence, fruits, and instrumentalities of violations of state and/or federal law. By this Affidavit and application, I respectfully request that the Court issue a search warrant directed to Verizon Wireless, allowing agents to seize the electronic communications and other information stored on Verizon Wireless computer systems and computer servers for the phone number [REDACTED] and the associated files described above.

For these reasons, I request authority to seize all electronic communications and other content stored in the Target Account, to be searched off-site in a controlled environment. Law enforcement officers and agents will review the records sought by the search warrant and will segregate any messages and content constituting evidence, fruits or instrumentalities of violations of state and/or federal criminal law. Additionally, I request authority to serve the warrant on the Verizon Wireless by facsimile and to allow Verizon Wireless to copy the data outside of this officer's presence.

  
Special Agent Jeff Kollars  
Division of Criminal Investigation

Subscribed and sworn to before me this 12 day of March, 2020.

  
(Notary Public)  
My commission expires 9/15/23

