FEDERAL BUREAU OF INVESTIGATION
FOI/PA DELETED PAGE INFORMATION SHEET
FOIPA Request No.: 1367178-000
Civil Action No.: 17-cv-01039-CRC

Total Withheld Page(s) = 67

<table>
<thead>
<tr>
<th>Bates Page Reference</th>
<th>Reason for Withholding (i.e., exemptions with coded rationale, duplicate, sealed by order of court, etc.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EFF-131</td>
<td>b6/b7C-3; b7D-1, 4</td>
</tr>
<tr>
<td>EFF-132</td>
<td>b6/b7C-3; b7D-1, 4</td>
</tr>
<tr>
<td>EFF-135</td>
<td>b7D-3; b7E-2</td>
</tr>
<tr>
<td>EFF-136</td>
<td>b7D-3; b7E-2</td>
</tr>
<tr>
<td>EFF-137</td>
<td>b7D-3; b7E-2</td>
</tr>
<tr>
<td>EFF-138</td>
<td>b7D-3; b7E-1, 2</td>
</tr>
<tr>
<td>EFF-139</td>
<td>b7D-3; b7E-2</td>
</tr>
<tr>
<td>EFF-140</td>
<td>b7D-3; b7E-1, 2</td>
</tr>
<tr>
<td>EFF-141</td>
<td>b7D-3; b7E-1, 2</td>
</tr>
<tr>
<td>EFF-142</td>
<td>b7D-3; b7E-2</td>
</tr>
<tr>
<td>EFF-143</td>
<td>b7D-3; b7E-1, 2</td>
</tr>
<tr>
<td>EFF-144</td>
<td>b7D-3; b7E-2</td>
</tr>
<tr>
<td>EFF-145</td>
<td>b7D-3; b7E-1, 2</td>
</tr>
<tr>
<td>EFF-146</td>
<td>b7D-3; b7E-2</td>
</tr>
<tr>
<td>EFF-147</td>
<td>b7D-3; b7E-1, 2</td>
</tr>
<tr>
<td>EFF-148</td>
<td>b6/b7C-1; b7D-3; b7E-2</td>
</tr>
<tr>
<td>EFF-149</td>
<td>b6/b7C-1; b7D-3; b7E-2</td>
</tr>
<tr>
<td>EFF-150</td>
<td>b7D-3; b7E-2</td>
</tr>
<tr>
<td>EFF-151</td>
<td>b7D-3; b7E-2</td>
</tr>
<tr>
<td>EFF-152</td>
<td>b7D-3; b7E-2</td>
</tr>
<tr>
<td>EFF-153</td>
<td>b7D-3; b7E-1, 2</td>
</tr>
<tr>
<td>EFF-154</td>
<td>b7D-3; b7E-2</td>
</tr>
<tr>
<td>EFF-155</td>
<td>b7D-3; b7E-1, 2</td>
</tr>
<tr>
<td>EFF-156</td>
<td>b7D-3; b7E-2</td>
</tr>
<tr>
<td>EFF-157</td>
<td>b7D-3; b7E-1, 2</td>
</tr>
<tr>
<td>EFF-158</td>
<td>b7D-3; b7E-2</td>
</tr>
<tr>
<td>EFF-159</td>
<td>b7A-1; b7D-3; b7E-1, 2</td>
</tr>
<tr>
<td>EFF-160</td>
<td>b7D-3; b7E-2</td>
</tr>
<tr>
<td>EFF-161</td>
<td>b7D-3; b7E-2</td>
</tr>
<tr>
<td>EFF-162</td>
<td>b7A-1; b7D-3; b7E-1, 2</td>
</tr>
<tr>
<td>EFF-163</td>
<td>b7D-3; b7E-2</td>
</tr>
<tr>
<td>EFF-164</td>
<td>b7A-1; b7D-3; b7E-1, 2</td>
</tr>
<tr>
<td>EFF-165</td>
<td>b6/b7C-6; b7D-3; b7E-2</td>
</tr>
<tr>
<td>EFF-166</td>
<td>b7D-3; b7E-2</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>EFF-168</td>
<td>b6/b7C-1, 3; b7D-4; b7E-2</td>
</tr>
<tr>
<td>EFF-169</td>
<td>b6/b7C-1, 3; b7D-4; b7E-2</td>
</tr>
<tr>
<td>EFF-170</td>
<td>b6/b7C-1, 3; b7D-4; b7E-2</td>
</tr>
<tr>
<td>EFF-171</td>
<td>b6/b7C-1, 3; b7D-4; b7E-2</td>
</tr>
<tr>
<td>EFF-172</td>
<td>b6/b7C-1, 3; b7D-2, 3, 4; b7E-1, 2, 5</td>
</tr>
<tr>
<td>EFF-173</td>
<td>b7D-3; b7E-2</td>
</tr>
<tr>
<td>EFF-174</td>
<td>b6/b7C-1; b7E-2</td>
</tr>
<tr>
<td>EFF-175</td>
<td>b7D-3; b7E-2</td>
</tr>
<tr>
<td>EFF-176</td>
<td>b7E-2</td>
</tr>
<tr>
<td>EFF-177</td>
<td>b7D-3; b7E-2, 5</td>
</tr>
<tr>
<td>EFF-178</td>
<td>b6/b7C-1, 3; b7D-4; b7E-2</td>
</tr>
<tr>
<td>EFF-179</td>
<td>b6/b7C-1, 3; b7D-4; b7E-2</td>
</tr>
<tr>
<td>EFF-180</td>
<td>b6/b7C-1, 3; b7D-2, 3, 4; b7E-1, 2, 5</td>
</tr>
<tr>
<td>EFF-181</td>
<td>b6/b7C-1, 3; b7D-3, 4; b7E-2</td>
</tr>
<tr>
<td>EFF-182</td>
<td>b6/b7C-3; b7D-4; b7E-2</td>
</tr>
<tr>
<td>EFF-183</td>
<td>b7D-4; b7E-2</td>
</tr>
<tr>
<td>EFF-184</td>
<td>b6/b7C-1; b7D-4; b7E-2</td>
</tr>
<tr>
<td>EFF-185</td>
<td>b7D-4; b7E-2</td>
</tr>
<tr>
<td>EFF-186</td>
<td>b6/b7C-1, 3; b7D-4; b7E-2</td>
</tr>
<tr>
<td>EFF-193</td>
<td>b7D-1, 4</td>
</tr>
<tr>
<td>EFF-194</td>
<td>b7D-1, 4</td>
</tr>
<tr>
<td>EFF-195</td>
<td>b7D-1, 4</td>
</tr>
<tr>
<td>EFF-196</td>
<td>b7D-1, 4</td>
</tr>
<tr>
<td>EFF-197</td>
<td>b7D-1, 4</td>
</tr>
<tr>
<td>EFF-198</td>
<td>b6/b7C-3; b7D-1, 4</td>
</tr>
<tr>
<td>EFF-204</td>
<td>b7D-1, 4</td>
</tr>
<tr>
<td>EFF-208</td>
<td>b7D-1, 4</td>
</tr>
<tr>
<td>EFF-209</td>
<td>b7D-1, 4</td>
</tr>
<tr>
<td>EFF-210</td>
<td>b7D-1, 4</td>
</tr>
<tr>
<td>EFF-211</td>
<td>b7D-1, 4</td>
</tr>
<tr>
<td>EFF-212</td>
<td>b7D-1, 4</td>
</tr>
<tr>
<td>EFF-232</td>
<td>b6/b7C-3, 7; b7D-4</td>
</tr>
<tr>
<td>EFF-233</td>
<td>b6/b7C-3, 7; b7D-4</td>
</tr>
</tbody>
</table>
FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE                                      Date: 01/18/2012
To: Los Angeles                                          Attn: Santa Ana RA, Squad CY-6
                                            SA Cynthia Kayle
From: Louisville                                          
      Squad 10                                             
      Contact: SA Tracey L. Riley,

Approved By: Dallas Mark J
Drafted By: Riley Tracey L:tlr
Case ID #: 
Title: INNOCENT IMAGES-LS
       UNDERCOVER GROUP II

Synopsis: To provide evidence and details regarding MARK
RETTEMAIER, 25462 Rodeo Circle, Laguna Hills, CA 92653, to the
Santa Ana RA, Los Angeles Division.

Package Copy: Being forwarded under separate cover is a 1
terabyte Seagate hard drive, Serial # 9TE243V2.

Enclosures: One, 1-A containing a copy of the Receipt of Property
(PD-597) and copies of the GEEK Squad Service Order/Terms of
Service, and a copy of the receipt generated buy Best Buy located
at 14395 Pipeline Ave, Chino, CA.

Details: On January 5, 2012, a CHS contacted SA Riley and
advised that Best Buy/Geek Squad had received a hard drive for
data recovery repair that contained suspected images of child
pornography. Best Buy/Geek Squad has a computer repair/data
recovery center located at 345 International Boulevard, Suite
300, Brooks, Kentucky 40109, 502-955-3800. All computers
received at Best Buy stores nationwide are sent to this facility
for data recovery.

On January 6, 2012, SA Riley personally visited the
Kentucky Best Buy/Geek Squad facility and spoke to the CHS.
The individual who requested the repair work is:

MARK RETTENMAIER
25462 Rodeo Circle
Laguna Hills, CA 92653
Primary Phone: 949-705-9015
Alternate Phone: 949-831-1624

The CHS advised that the questionable images were observed after the data recovery repair had been made for images. In order for the technician to determine that the repair was successful they must access the files to verify that the files were recovered intact. In the course of ensuring the repairs were successful the Best Buy/Geek Squad technician began by performing a search for pictures and/or jpegs. As the Best Buy/Geek Squad technician was scrolling through the thumbnails he observed the images he suspected were child pornography. The technician then contacted the CHS, who contacted SA Riley and secured the hard drive.

It should be noted that SA Riley observed the images that the Best Buy/Geek Squad technician observed. Because it was immediate obvious that there were known CP images, SA Riley seized the hard drive.

While at the Geek Squad a known image of "9yo Jenny" was immediately observed by SA Riley. This particular image was of a fully nude, white, prepubescent female on her hands and knees on a bed, with a brown choker type collar around her neck.

Once back at the Louisville office the hard drive was attached to a forensic write blocker, a scan was performed with a preview tool. It was determined that the data on the hard drive is underlying, meaning that a scan needs to be done for formatted files using a forensic tool that carves jpg images. Since the Geek Squad uses tools similar to forensic tools used by the FBI's RCFIs it is not possible to view images without using a forensic tool to carve the images.

The hard drive was then placed into evidence at the Louisville office of the Federal Bureau of Investigation.
SA Riley understands that every United States Attorney's Office has different prosecution thresholds. If it is determined that these images do not rise to that level, and no investigative action is taken by the Los Angeles Division, the Geek Squad/Best Buy requests that the hard drive be returned to them in Kentucky so they are able to complete their processes.

Please note item 8 under the "I agree to/or that" section on the Service Order form states that the customer is "on notice that any product containing child pornography will be turned over to the authorities". Please contact SA Riley if there are any additional questions.
LEAD(s):

Set Lead 1: (Action)

LOS ANGELES

AT LAGUNA HILLS, CALIFORNIA

Los Angeles is requested to review the hard drive and documents enclosed for case potential. If no case is opened please return the hard drive to the Geek Squad located in Kentucky.

* * *
Title: (U) Telephone call with SA Riley.  

Date: 02/20/2015  

From: LOS ANGELES  
LA-OCR1 SSA  
Contact: KAYLE CYNTHIA,  

Approved By: A/SSA  

Drafted By: KAYLE CYNTHIA  

Case ID #: 305D-LA-259472  
(U) RETTENMAIER, MARK - MARK RETTENMAIER  

Synopsis: (U) Telephone call with SA Riley.  

Full Investigation Initiated: 01/23/2012  

Details:  

On 02/17/2015, SA Kayle spoke with SA Riley by phone. SA Riley advised she made a request to headquarters in order to locate any emails between her and Best Buy regarding the above titled case. SA Riley advised that she had opened a Best Buy employee in a supervisory position as a confidential human source (CHS).  

On 02/19/2015, SA Kayle spoke with SA Riley by phone. SA Riley advised she has not yet received a response from headquarters regarding her email account. SA Riley reiterated the CHS she opened at Best Buy was due to agent requirements and the CHS was not a traditional source. SA Riley believes he/she has been closed for approximately two (2) or three (3) years.
UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION
Electronic Communication

Title: (U) Copy of Email Chain.                       Date: 03/02/2015

From: LOS ANGELES
      LA-OCR1 SSA [Redacted]
      Contact: KAYLE CYNTHIA, [Redacted]

Approved By: SSA [Redacted]

Drafted By: KAYLE CYNTHIA

Case ID #: 305D-LA-259472 (U) RETTENMAIER, MARK - MARK RETTENMAIER

Synopsis: (U) Copy of Email Chain.

Full Investigation Initiated: 01/23/2012

Enclosure(s): Enclosed are the following items:
1. (U) email chain

Details:

Enclosed for the file is a copy of the email chain from a Best Buy employee to SA Riley.

♦♦♦

UNCLASSIFIED
Title: (U) Lead to Louisville, KY. 

Date: 03/25/2015

From: LOS ANGELES
LA-OCR1 SSA

Contact: KAYLE CYNTHIA

Approved By: A/SSA

Drafted By: KAYLE CYNTHIA

Case ID #: 3050-LA-259472 (U) RETTENMAIER, MARK - MARK RETTENMAIER

Synopsis: (U) Lead to Louisville, KY.

Full Investigation Initiated: 01/23/2012

Details:

Reference telcall with SA Tracey Riley on 03/24/2015, Los Angeles is requesting a copy of CHS file [REDACTED] to include CHS's identifying information.

+++
JUSTIN MEADE, "telephone number" was interviewed by telephone, by Special Agent Cynthia Kayle, and Assistant United States Attorney Anthony M. Brown. After being advised of the identity of the interviewing Agent and the nature of the interview, MEADE provided the following information:

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency, it and its contents are not to be distributed outside your agency.
Title: (U) Copy of CHS documents from Kentucky. Date: 04/15/2015

From: LOS ANGELES
LA-OCR1 SSA
Contact: KAYLE CYNTHIA

Approved By: SSA

Drafted By: KAYLE CYNTHIA

Case ID #: 305D-LA-259472 (U) RETTENMAIER, MARK - MARK RETTENMAIER

Synopsis: (U) Copy of CHS documents from Kentucky.

Full Investigation Initiated: 01/23/2012

Enclosure(s): Enclosed are the following items:
1. (U) copies of CHS file

Details:

On 4/6/2015, writer received the enclosed documents from FBI Louisville, KY. The documents are copies of the entire CHS file

UNCLASSIFIED
**FEDERAL BUREAU OF INVESTIGATION**

**PAYMENT REQUEST**

---

**DRAFT TYPE**

- Request Type: [Blank]
- Payment Type: Confidential
- Forfeiture or Drug Related: No

---

**INFORMATION ABOUT THE REQUESTING EMPLOYEE**

- Official Bureau Name: [Blank]
- Social Security Number: [Blank]
- Date of Request: 08/05/11
- Field Office: [Blank]
- Squad: [Blank]
- Cost Center: [Blank]
- Telephone Number: [Blank]
- Louisville: X

---

**INFORMATION ABOUT THE REQUESTED PAYEE**

- Payee Name: [Blank]
- Social Security or Taxpayer ID Number: [Blank]
- Burghley

---

**Is this a one-time non-salary source payment?**

- No

---

**Source Number**

- [Blank]

---

**Serial Number**

- [Blank]

---

**Payment Name**

- [Blank]

---

**Date of Approved Waiver Request**

- 10/01/10

---

**Period Covered From**

- 09/30/11

---

**Period Covered To**

- 09/30/11

---

**Financial Justification:**

- [Blank]

---

**DETAILS ABOUT THE REQUESTED DRAFT**

<table>
<thead>
<tr>
<th>Fiscal Year</th>
<th>SOC</th>
<th>Incurred by Agent or CHS</th>
<th>Catalog</th>
<th>File No.</th>
<th>Comanche Program/Subprogram</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CHS Expense</td>
<td>$500.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Description: Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Total For</td>
<td>$500.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Total</td>
<td>$500.00</td>
</tr>
</tbody>
</table>

---

**OBLIGATION PROCESSING**

<table>
<thead>
<tr>
<th>Vendor Number</th>
<th>Group Number</th>
<th>Obligation Number</th>
<th>Follow up Date</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Document Number</th>
<th>Payment Reference Number</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Signature of Cashier.</th>
<th>Date.</th>
</tr>
</thead>
</table>

---

**SETTLEMENT OF ADVANCE**

- Prior Month Advance Balance: [Blank]
- This Advance: [Blank]
- Less Receipts: [Blank]
- Funds Returned and/or Cash on Hand: [Blank]
- Amount to be Reimbursed: [Blank]

---

**EXPENSE PROCESSING**

<table>
<thead>
<tr>
<th>Document Number</th>
<th>Draft Number</th>
<th>Signature of Cashier</th>
<th>Date</th>
</tr>
</thead>
</table>

---

**APPROVAL**

- Name: [Blank]
- Date/Time: [Blank]

*Approved By SSA:*

- Dallas, Mark J

*Certified by ASAC:*

- [Blank]
- 9/1/2011 2:39:23 PM

*Draft Approval Officer:*

- [Blank]
UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

To: Louisville

From: Louisville
   Squad 10
   Contact: SA Tracey L. Riley,

Approved By: 

Drafted By: Riley Tracey Lt:lr

Case ID #: (Pending)

Title: 

Synopsis: To request SSA approval for the initiation and continuation of e-mail contact with Confidential Human Sources (CHS).

Details: Per the FBI's CHS Policy Manual, SSA approval is required for the initiation and continuation of all e-mail contact with CHS's. This approval must be obtained and documented in the CHS's main file.

CHS [_____] and CHS [_____] has a preexisting, overt relationship with the FBI. Overt email communication is used for coordinating meetings, or in some cases asking for the status of their product.

++

UNCLASSIFIED
UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION
Electronic Communication

Title: (U) Tentative suppression hearing date

From: LOS ANGELES
LA-OCR1 SSA
Contact: 

Approved By: SSA 

Drafted By: 

Case ID #: 305D-LA-259472 (U) RETTENMAIER, MARK - MARK RETTENMAIER

Synopsis: (U) Defense counsel suggested a mid-November date for the suppression hearing therefore AUSA Greg Scally requested status of potential witnesses.

Full Investigation Initiated: 01/23/2012

Details:

On August 31, 2015, Assistant United States Attorney (AUSA) Greg Scally emailed Special Agent (SA) _______ and advised that defense counsel suggested a mid-November date for the suppression hearing. Therefore, AUSA Scally requested SA _______ to inquire about the availability for the following potential government witnesses:

SA Cynthia Kayle

SA Tracey Riley

SA _______

Task Force Officer (TFO) Seal Beach Police Department

Field Examiner (FE) Orange County Regional Computer Forensic Laboratory

Justin Meade, Best Buy employee

UNCLASSIFIED
On August 31, 2015, SA Riley emailed SA[Redacted] and advised that she does not have any trials scheduled in November. Her availability was provided to USA Scally.

On August 31, 2015, TFO[Redacted] texted SA[Redacted] and advised that he is teaching at the police academy on November 5 and November 11 and is out of state from November 18 to November 25, 2015. His availability was provided to USA Scally.

On August 31, 2015, SA Kayle telephonically contacted SA[Redacted] and advised that she has no conflicts in mid-November. Her availability was provided to USA Scally.

On August 31, 2015, SA[Redacted] telephonically contacted Justin Meade and left a voicemail inquiring about his availability in mid-November.

On September 1, 2015, Meade returned SA[Redacted] call and advised that he has no conflicts in November. However, since he works in retail, Meade expressed his hopes that the hearing would be scheduled earlier rather than later in November as retailers become busier as Christmas nears. SA[Redacted] inquired if Meade had any prior contact with Trey Westphal in any social media platforms to include, but not limited to, LinkedIn, Instagram, etc. Meade advised that he would check his various accounts to see if he had any contact information for Westphal. Meade’s availability was provided to USA Scally.

On September 1, 2015, SA[Redacted] telephonically contacted SA[Redacted] and advised that he has no conflicts in mid-November. His availability was provided to USA Scally.
Title: (U) Notes from Phone Call with Tracey Riley.

Date: 12/17/2015

From: LOS ANGELES
    LA-OCR1 SSA
    Contact: KAYLE CYNTHIA,

Approved By: A/SSA

Drafted By: KAYLE CYNTHIA

Case ID #: 3050-LA-259472 (U) RETTENMAIER, MARK - MARK RETTENMAIER

Synopsis: (U) Notes from Phone Call with Tracey Riley.

Full Investigation Initiated: 01/23/2012

Enclosure(s): Enclosed are the following items:
1. (U) Notes

Details:

Enclosed for the LA section of this file are notes from the phone conversation with SA Tracey Riley on 12/17/2015.

♥♥

UNCLASSIFIED
After seeing motion picture, Tracy thought they must be notes & went looking in a file cabinet.

Chris: Sunday a.m., we'd known.
Friday copy of EC + hand written notes.
Had to be looking at data from hard drive.

Mike standing at tale at 6th Street.
Unable to open anything at 6th Street. Some notes may be from when she looked at Best Buy.

Maybe Justin needs to call @ scaled # to come to Best Buy.

She only recognizes name based on paperwork (note) they gave her.

She never contacted Tracy/never directed anyone at Best Buy to look for CP.

Never signed Tracy as chs.

Tickets don't always say when Tracy is called. She can't recall if they were there.

She believes the person who contacts her is in a supervisory role.

Justin would have picked her up at front desk. Brought her to store to look, not allowed to walk around by herself.

No question what she saw was CP.

Twisted up appears yrs. new.

Partial image could not be in frame or had pinched.

Signaled Justin as chs to satisfy Fire policy.
Best Buy is a watch contract.

System in paper, they can do what a server does: play.

Can't do EC, only keyboard.

This is a way to keep a paper trail indefinitely.
She recognized the tiny scenes, seen around since 2002.

Somehow, in prior investigations,

familiar with V. K. and know it was identified scenes

with a real girl.

Never been implicated for anything incriminating

with source. Supervisor is unaware of all calls

documents, they sign off.

She recalls talking calmly in the phone after

initial lead.

Need to have had the notes in front of her

when she called me.

At the time of the phone call she didn't remember

having notes.

They pull up a screen, whatever is there is there.

The most she would do is click on an image to

make it bigger. She doesn't scan or scroll down.

Did not ask them to acquire files.

She doesn't touch anything. No search anything.
Title: (U) Notes of Phone Call with Justin Meade. Date: 12/31/2015

From: LOS ANGELES
LA-OCRI SSA
Contact: KAYLE CYNTHIA, 

Approved By: A/SSA

Drafted By: KAYLE CYNTHIA

Case ID #: 305D-LA-259472 (U) RETTENMAIER, MARK - MARK RETTENMAIER

Synopsis: (U) Notes of Phone Call with Justin Meade.

Full Investigation Initiated: 01/23/2012

Enclosure(s): Enclosed are the following items:
1. (U) notes of phone call

Details:

Enclosed for the IA section of the file are the notes from the phone call with Justin Meade, AUSAs Tony Brown and Greg Scally, and SA Cynthia Kayle, on 12/30/2015.

***
Title: (U) Emails with Justin Meade and Trey Westphal

From: LOS ANGELES
LA-OCTR SSA [Redacted]
Contact: KAYLE CYNTHIA, [Redacted]

Approved By: SSA [Redacted]

Drafted By: KAYLE CYNTHIA

Case ID #: 305D-LA-253472 (U) RETTENMAIER, MARK - MARK RETTENMAIER

Synopsis: (U) Emails with Justin Meade and Trey Westphal

Full Investigation Initiated: 01/23/2012

Enclosure(s): Enclosed are the following items:
1. (U) Justin Meade and Trey Westphal emails

Details:

Enclosed for the file are emails with Justin Meade and Trey Westphal.

† †
Kayle, Cynthia (LA) (FBI)

From: Justin Meade
Sent: Thursday, January 14, 2016 12:38 PM
To: Kayle, Cynthia (LA) (FBI)  
Subject: Re: New Hearing Date

Should not be a problem thank you for the update.

On Thursday, January 14, 2016, Kayle, Cynthia (LA) (FBI) wrote:

Justin,

AUSA Scally just advised the new hearing date is set for Monday, May 23, 2016, at 9:00 a.m. The U.S. Attorney’s Office will contact you to plan travel arrangements. Please call me if you have any questions.

Thanks,

Cynthia

Justin Meade
S.A. Kayle,

Thank you for the update, I will update my request at work to reflect the new date and make travel arrangements accordingly.

Best regards,
Trey

On Thursday, January 14, 2016, Kayle, Cynthia (LA) (FBI) wrote:

Trey,

AUSA Scally advised the new hearing date is Monday, May 23, 2016, at 9:00 am. The U.S. Attorney’s Office will contact you to plan travel arrangements. Please call me if you have any questions.

Thank you,

Cynthia
JUSTIN MEADE (MEADE) was interviewed by telephone. Assistant United States Attorney (AUSA) Anthony Brown and AUSA Greg Scally were present on the phone call. After being advised of the identity of the interviewing Agent and the nature of the interview, MEADE provided the following information:

Investigation on 04/06/2016 at Orange, California, United States (Phone)

File # 305D-LA-259472 Date drafted 04/06/2016

by RAYLE CYNTHIA

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.
JUSTIN MEADE (MEADE), was interviewed by telephone. Also present on the phone call were Assistant United States Attorneys Greg Scally and Anthony Brown; and General Counsel for Best Buy. After being advised of the identity of the interviewing Agent and the nature of the interview, MEADE provided the following information:
Does not remember this email.

He was a General Manager

Justin was more hands-on & day

was Justin's manager. Randall was

man of a standing. Remembers Tracey

Doesn't remember her name. David's

Doesn't remember Tracey returning to DB

on a case. Lots of times he doesn't

didn't know she was there. He looked up

high, Justin would come get it. If POI

took it, he would get record & file it.

Doesn't think Tracey would have notes or record.

Tracey coming back on re-hearsal.

If you saw something questionable

they would stop immediately.
ID would be locked up until Fox came to look. If not it (questionable).

The tech would get ID back + continue data recovery.

If ID seized BB doesn't retain copy
Some data stored on phones. May have been stored for 30 days then purged.
Justin if they would have to answer that. He's just a manager.

No recollection of Fox re-recovery images.

They didn't look for certain things.

Pushkids came on screen to check

Cowboy tells unclear to decide

They were just to stop

Safe in a locked room.

Not sure if Justin had cancer.
Male FBI agent prior to trial:
Absolutely not - no FBI agent ever asked or directed him to search the file. Not to open any files not needed for the job.
Doesn't remember. They wished it.
Not in data recovery, just in repair shop.
Wishers would open laptop and see pic of good looking girl + employee wants to see their pics. That employee would be fired. Not to be related.

Justin Davis didn't contact the FBI.
Him didn't contact FBI.

FBI didn't pay him to find evidence or CP.

Doesn't remember CP burner.
None of the employees that did the work dealt with FBI. It was supervisors.

Left around May 2013.
Mill hands - whole Ewing affair before
Dwy. Had some contact with FBI
or something.

Never told techs to search
for evidence for FBI. Sure that
Justin or Hill wouldn't have
done that.

Techs knew it was a derelict
offense as they worked outside the
Scope of juv. knew people were
drank. Didn't want to tarnish their
reputations.
9/21/16

Michael H. - did not work together, know name, never met
- does not recognize name

- DRD - data recovery dept.
  - peers, then was pseudo supervisor
  - became manager
- direct to search for CP? - No

- nobody in company ever asked to search for CP on any device that he worked on

- never been asked by FBI / BB Geek
- only instruction - search for items identified as important by client
  - default, pictures, documents, music, etc.

- not aware of anyone at company being instructed
- name sounds familiar, not sure

su aware of a Sup 1st shift

Randall Ratliff
Assistant Area Manager

Justin Mende
orig 2nd shift manager

Dong Manager

Currently not working at Best Buy
Title: (U) Notes of Phone Conversation with Jennifer Cardwell

Date: 11/28/2016

From: Los Angeles
LA-OCR1 SSA
Contact: Kayle Cynthia

Approved By: SSA

Drafted By: Kayle Cynthia

Case ID #: 305D-LA-259472 (U) Rettenmaier, Mark - Mark Rettenmaier

Synopsis: (U) Notes of Phone Conversation with Jennifer Cardwell

Full Investigation Initiated: 01/23/2012

Enclosure(s): Enclosed are the following items:
1. (U) Notes

Details:

Enclosed for the file are handwritten notes of a conversation with Jennifer Cardwell on 07/12/2016.

**

UNCLASSIFIED
Jennifer Cardwell 7/12/14
She vaguely remembers Justin Head. She didn't have that much interaction with best but current co-worker. Did go to TBS a couple times. Never asked him to do anything extra just in the course of your duty to all, never directed with to search for DP or any evidence.

2/2010 Trust off Squad
needed to have a source on the books

Collabo - definitely not anything illegal or any idea for looking for info.
telephone number was interviewed by telephone by Special Agent Cynthia Kayle and Assistant United States Attorneys Anthony Brown and Greg Scally. After being advised of the identity of the interviewing Agents and the nature of the interview, provided the following information:

was emailed two (2) documents; Bates 852-855 and Bates 59. was asked about the entries in the log that appeared to be documented by him.

stated in November 2011, he was in the data recovery department. stated he basically "did it all." did imaging, etc. was employed in that department for approximately seven (7) years.

stated on the first form he recognized his handwriting for the percentage 7.75% and voice. stated when the drive was diagnosed, he looked up the sales tax rate and noted that a voice waiver was needed. advised the FR-crash scanning may have been from format recovery. stated mule 17 is most likely because the recovery went to Mule 17. Nothing on this form indicates to that child pornography was found.

stated that as part of the service request the technician was to diagnose the drive, but not to do recovery as they need a voice waiver or they need the customer to stop in to the store and do a waiver.

stated the log entry 11/28/2011 09:09:06 PM contains his employee number in the third column stated he doesn't have a way to know if the files were unallocated or not. stated it's common sense to tell if a drive appears to be restored. stated MFT records mean to look for as much data on the drive as possible. advised data carves are the best effort to get the data back. stated using F11 can restore a computer and basically put it back in a manner in which it came out of the box when it was new. It's an attempt to be brought back. stated in the log entry "drive appears to have been restored" means it appeared someone (either the customer or the previous Best Buy department) restored the drive. Again stated this means restoring the computer basically to the way it was when it came out of the box.
remembered the drive was beginning to fail. stated if that happens to a drive, he wouldn't want to kill the drive, so he would image to a new drive and try the recovery on that imaged drive.

is unaware if Best Buy or the customer did anything to the drive before he received it.

stated a Level 2 ADV IGMFT is for files deleted and to look for all possible files even if they are unallocated.

stated underlying data visible is because the disk gave the impression there was more data. used a hexadecimal view where he can see numbers and letters the way the computer reads it. can't see the actual data; pictures or files, but in one particular view may be able to see file names.

stated by dragging back and forth across the drive he is able to see how much space is on the drive and make a determination that there appears to be underlying data.

stated there is no entry on the log that indicates he or anyone else located child pornography.

stated there was only one case where he saw child pornography, but he doesn't know what case it was. remembers he was checking to see if files were restored and going through the results and saw images.

stated that process would not have been at the early stage that his log entry was in this particular case.

stated that no process was undertaken that shouldn't have been done prior to the voice waiver. stated his log notes at 09:09:06 are diagnosis notes and not data recovery. stated it's necessary to run checks and plug the drive in to diagnose it.

stated his job was to diagnose the drive and then move on to the next drive. There is no indication of data recovery. stated he was not assigned this drive for the entire process.

stated he saw FBI Agents at his work, but he didn't talk to them. stated no FBI Agent ever directed him to search for child pornography.

recalled there were employee meetings from time to time where the employees were told not to search for things, but if they saw anything like this to report it to the boss. doesn't remember who ran the meeting.
305A-LA-259472
Continuation of 305A of [Redacted] Interview of [Redacted].
On 12/13/2016. Page 3 of 3

[Redacted] stated Doug Christophel (Christophel) and Justin Meade (Meade) were bosses. [Redacted] stated Christophel and Meade never told him to search computers for child pornography. [Redacted] stated nobody ever told him to search computers.

[Redacted] advised [Redacted] Trey Westphal (Westphal) on a device when he saw what he thought was child pornography. [Redacted] does not know if it was this case. [Redacted] recalls he worked in advanced recovery and

recalls seeing images and thumbnails, some of which were damaged. [Redacted] saw an image of a younger individual. [Redacted] doesn’t recall what happened next. [Redacted] doesn’t remember writing anything. [Redacted] stated it was a page of thumbnails but he zeroed in on one image and got spooked so he stopped. [Redacted] doesn’t know what was submitted to the bosses. [Redacted] stated the document he was shown that was written by Westphal is indicative of a similar diagnosis.

[Redacted] stated he never heard any Best Buy employees discuss searching hard drives outside of the scope of the data recovery process.

[Redacted] stated he was

[Redacted] was asked if he knew the following people:

- [Redacted] stated he was a

- [Redacted] stated he may be

- [Redacted] stated she may be a

- [Redacted] knows him

Michael Han - [Redacted] stated he’s an equal to Christophel

- [Redacted] doesn’t know him

Trey Westphal - [Redacted] stated he knows him.

[Redacted] stated none of the above people ever told him to search for child pornography.
3 different clients at least 3 calls.

23 weeks prior to showing up at 1AM tracked him down at the
WTC infirmary about Best Buy data
recovery.

Saw a fat Asian guy named Vito
Supervisor.

Deemed we need a way to know if
it was allocated or not.

And another says while with
Vito. varsity: his handwriting.

Ship parity = directly by
service center tracking - inventory control of
customer accounts.

A's - account

B - branch

C - customer

D - data recovery dept

T - tracking of

This did just about everything.
Additional view doesn't show the actual story.

For EST - Recovery estimate, we'll have diagnostic tooling. It will see how much space is needed.

Any way that shows he had CP?

Only saw 1 case where he saw CP. He doesn't know what case we need it for. Saying something.

Maybe in other CP case.

Nothing to suggest it didn't restart; giving strength tests a basic image wouldn't have been at this early stage.

Anything in this log that indicates what happened at all this ID?

Log entry 1:31:02

Pre-crash scanning may have hang from General Recovery.

Someone's saying it's hard to make a reality that this firm indicates that someone

Any process undertaken with shutdown have been done with shutdown's ID.

Request rules on ACME not data recovery.
The document appears to be a list of bullet points and a few paragraphs. Here is a transcription:

- Process: Diagnosis - when and to another employee for data recovery.
- Never heard anyone discuss searching hardware devices before for data recovery.
MIKE HANS (HANS), telephone number ___________________________ home address ___________________________

email address ___________________________

was interviewed by telephone. Also present for the interview was Assistant United States Attorney Greg Scally. After being advised of the identity of the interviewing Agent and the nature of the interview, HANS provided the following information:

Investigation on 12/28/2016 at Orange, California, United States (Phone)

File # 395G-1A-259472

Date drafted 12/28/2016

by KAYLA CYNTHIA

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and it and its contents are not to be distributed outside your agency.
UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION
Electronic Communication

Title: (U) Interview notes (typed) of

Date: 11/03/2017

From: LOS ANGELES
LA-CCRI SSA
Contact: KAYLE CYNTHIA,

Approved By: A/SSA

Drafted By: KAYLE CYNTHIA

Case ID #: 305D-LA-259472 (U) RETTENMAIER, MARK - MARK RETTENMAIER

Synopsis: (U) Interview notes (typed) of

Enclosure(s): Enclosed are the following items:
1. (U) Typed notes of phone interview of

Details:

Enclosed for the file are the typed notes of the phone interview of
on 12/30/2016.


UNCLASSIFIED

EFF-234
Best Buy, 345 International Blvd, Brooks, KY 40109. 12/30/16 Scally, Brown

9/25/99 at store before moving here.

Was there in 2011 and 2012. Always in the facility. Came down in late 2007. Might have been in a different department that time but familiar with processes of data recovery.

How units get to Geek Squad City and what it is:

Repair facility and handle different types of operations including data recovery. Repair computers is goal. Initiated by client at store. Whether repair or data recovery they are requesting service to be performed then shipped to their facility to be performed.

Best buy geek squad policy for reporting CP – he’s familiar with policy and there’s documentation on that. Back in 2011 2012 was he familiar. It’s very similar to the process now but he doesn’t have the exact verbiage. SOP based on those same processes so should be very similar. Standard procedure is if somebody comes upon CP during the course of work they are instructed to immediately stop and instruct supervisor that they’ve encountered that. The supervisor then contacts law enforcement. Since units are nationwide their local law enforcement is the local FBI since they have jurisdiction across country. They call FBI, FBI responds and decides if they are going to take it and they find the proper paperwork for handoff and go from there.

Your direct management contacts the FBI. It’s the same throughout the facility regardless of department. If someone discovers CP, they stop and report it to supervisor.

He’s had contact with FBI agents over the years. Tracey another guy. They are contacted because they are in the local office. He was never asked to be an informant or CHS. Agents never asked him to search for CP. We don’t get involved any more after the handoff. Agents never paid or offered to pay him money in connection with his work at Geek Squad. Not aware of any employees who became informants. Not aware of any employees being paid by FBI.

(Reading Star Log)

Putting in info from client when first created. Name and phone number. First piece

Moving down it’s saying we collected a deposit of $249 and at that point that was a pre set amount that had to be attached to any unit that was requesting data recovery. Base price. Wouldn’t be shipped if they weren’t willing to pay at least $249. Data recovery would have been requested at this point because customer would have had to pay $249 which is a minimum charge that they have to agree to before shipping that here.
Shipment info the tracking to Geek Squad City. Some is automated status updates.

11/25 receiving and that’s showing it was received into the building, changed status awaiting customer info. That is going to take place in the department so it reached the data recovery center and it’s awaiting customer info status. Checked into work in progress. Staging for stuff that’s going to be worked on in data recovery.

Only a few statuses for star. Not designed for data recovery. Only a few things to show movement. Getting unit prepped for diagnosis to get info back to client. Star designed for repair. They’re not repairing hardware they’re recovering data.

(Why voice waiver if client already gave permission at beginning for data recovery) Service order gives permission to access the device for diagnosing the hardware. As long as diagnosing and some repairs that’s enough but when it comes to reviewing client’s data it’s more sensitive and they have to seek out and verify data and make sure they’re getting correct results. Because of sensitivity they require signed data services agreement or voice waiver to show that client gives permission for them to go through info on device.

Costing more money doesn’t necessarily mean they need a voice waiver, the waiver is because of the fact they will be going through the data. A lot of stuff is just for hardware repair and only needs original service order but data recovery is different and needs the voice waiver.

11/28 9:09 PM, it shows that we hooked it up and diagnosing drive to see what if any mechanical issues were going on, what it was going to take in order to access the data on that drive. Once we find that out we can provide client with estimate to recover that data. We are still awaiting the waiver because in order to go through data and verify they need the waiver. Shows the level of recovery, cost and awaiting waiver.

Level 2 advanced recovery some kind of damage to file system or something that is going to be required in order to even access data that isn’t going to be accessible just using standard Level 1 or 2 process. Maybe advanced corruption or boards to make the drive useful again falls under Level 2 advanced Igmft – master file table. Technique used during level 2 process to make data accessible. Person diagnosing and telling recovery agent what will be needed in order to finish out recovery. Appears some damage to master file table in this case.

Drive appears to have been restored means: When they’re doing the diagnosis a lot of tools can look at hex information and see what the condition of the drive is and see where data is missing even though we can’t see the data itself we can see where data was on the drive. Based on the layout that we see through the software we can see if the drive looks to have been formatted. May show up as all zeroes and everything gone, won’t be able to recover anything. This is done during diagnostic step and inform recovery agent this is where you’ll need to look to find data, these are some of the issues with the drive, etc. in order to get the best results what we get the approval.
Restored means: Does not mean the drive has been fixed already. HP recovery tools can restore or reformat back to factory settings. Can’t tell by log if it was Best Buy or client did restore, but would have been done before it reached Geek Squad. When we complete diagnosis it’s only going to give us a guestimate of what happened prior. Accidental issues could show up the same as if you formatted on purpose. We don’t know until the client says this is what I did.

IGMFT and drive appears to have been restored: kind of goes hand in hand. If there are problems with computer or problems led someone to restore unit we can see similar results with the diagnostic we have here.

Underlying data visible: Hex view. Hex data. Diagnostic tools show 1’s and 0’s and they know they should be able to get data because it’s underlying.

Underlying: If there was some corruption of master file and wouldn’t boot for client you would describe data as underlying because it’s inaccessible through normal means of the computer. Is that the same as unallocated space? No. that’s a little different. When a drive is set up it sets up different spaces o that drive for different things. Unallocated space if you format a drive for use you’re going to have some bit of unallocated space on a hard drive. The drive is sometimes split between reserved space for files, operating system and in that process will sometimes have unallocated space as well so it doesn’t necessarily mean there was a problem with formatting, but through formatting you can have some unallocated space. Unallocated by itself doesn’t necessarily mean something was formatted.

If you delete data on computer that data lies in unallocated space because computer put it in status where data can be overwritten with new data. Is that correct? Yes. It would do that.

If a master file table was corrupted in some way, that could make it look as if the data that used to be accessible to a computer user, it could make it look as if it’s in unallocated space. Yeah, the structure is gone at that point so you have a lot of files sitting loose on that drive. There’s nothing that directs you because the names are stripped away so everything is still there but you don’t know it because there’s no map anymore.

One doesn’t necessarily mean that the other happens, but sometimes in conjunction with each other because something got formatted now you may have unallocated space because of formatting, but one is not a requirement for the other.

In the log for that entry: That doesn’t indicate to you that the tech was viewing any type of content on the drive like actual files or pictures? No. The tools we typically use review hex data, it’s coded information. The 1’s and 0’s. It shows where data would be. Even if tools change, the way they work is the same.

Data underlying doesn’t mean data files themselves are visible? Right, we just know something is there and whether it’s worth it to try and recover data.
Any indication in entry that anything was done that shouldn’t have been done prior to voice waiver? No. It doesn’t go to recovery team until voice waiver and funds collected.

At diagnostic stage there is no risk to privacy because we’re only looking to see if data is there, not the actual data. There’s no one looking for CP at diagnostic stage? No, not at all. It is against Best Buy policy to be searching for anything. Not searching at any stage.

Policies in place and disciplinary action if it is deemed you are searching a customer’s computer. Everyone learns this through when they get onboarded. Small sampling from client’s mission critical list to make sure those pieces are functional. That’s why they have the waiver to let client know this is what we are going to be doing and they give permission. They need to verify they have good results. Privacy is a very important piece. If there was a way to do it another way they would do that.

11/28 where client recorded voice waiver and mission critical – most important files to client, pictures, excel, quicken, etc. when we complete that recovery that’s what we’ll key in on to make sure we’re getting results. They’re not going to put effort into other data.

Verify location of product through recovery process so they verify this product is where they expect it to be – binning audit.

12/19 the advanced recovery attempt failed. Bad blocks in drive – section of drive that hold data and was causing the recovery to fail. We went through and did a full image of the drive because if you have a bad drive, reading and writing data, we ran into problems with that so the best thing is to image which is less stressful on the drive and better results. The imaged to another working hard drive so they could then attempt to process the recovery. That’s Mule 224 (inventory number).

If a drive is failing and probably the reason he brought the drive in is because the drive was failing – bad blocks. So they use a different technique to get data onto working drive so they can complete a recovery. Different things cause data loss, hit delete, corrupt, format, and here we have data corruption due to failed hard drive. If they transfer to another drive the data is still corrupted and unreadable because drive corrupted it when it was failing. So image to Mule 224 is first step so we don’t have to worry about the drive failing and can then start the recovery process to make the data useful. Everything made it to the mule except for the small KB amount.

Completing the recovery using the techniques they use for drives that had been formatted and due to the fact the drive was failing that is the recovery that was required – format technique to recreate data and get it usable again.

12/20 review process must have run into CP because Randy Ratliff was the ambassador at the time. Doesn’t know TW or that signature from when he was working. Knows Randy. Was not aware Randy was an informant for the FBI.

528 document: Trey’s statement: data review of format recovery – when we complete a recovery we go through and review that data to make sure it was able to be put back into usable format and if we do it and it’s still garbage we’re not going to charge someone a recovery cost if the data is unusable. That’s
why we ask for mission critical so we can get back info client is looking for. If you ask for pics and we can only recover music, that’s a fail and we’re not going to charge you.

Kind, picture width: a lot of programs generate pics of some sort, the internet will generate thumbnails, itunes generates album art, generally very small. What happens is if you have a lot of that content it’s hard to differentiate pics from album art and pics you took pics of while on vacation so we narrow search down so we can focus on things you were actually taking pics of by getting rid of small thumbnails. 200 is likely kb because if you eliminate that you will filter out album art and get pics that are meaningful to you. Pics measured in kb but there could be other means of filtering that information out.

12/20 corresponds with Trey’s statement. We stop at the point and everything is hands-off. He’s been involved in process of bringing in law enforcement.

How are images displayed for agent? Typically we hand over the notes of this is what I was doing and how I did it and where I was and we hand over to FBI. They will go to secure area. We don’t want that viewed by anyone else around. Either in private conference room or clear out area of department and let them view it. Give over the notes and let the FBI handle the search.

Tony: Agent came back on 2/3 after seizing HD on 1/6. When she came back was she looking at content on imaged hard drive on Mule? Any insight into how that happened? I’m not sure. It would make sense because we will lock that service order up. The mule, the paperwork, looked up so it makes sense if they took hard drive that they wouldn’t be able to view because drive was faulty. Same problem they had when they tried to complete recovery so may have looked at data on Mule the image they created from original drive.

Anything on star log p856 after the entry from 12/20 that would indicate that the Mule that was used for the data recovery process in this case was placed into a safe location and there’s nothing in the log that shows that the Agent came down on 2/3 to look at mule.

Status change to complete – more than likely done to prevent that from continuing to show up in the queue. Otherwise questions would continue to arise on that.

Justin, Hans and Christophel were his supervisors at some point.