IN THE UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

NO. **09-10579-BB**

United States of America,

Appellee,

- versus -

Timothy Beckett,

Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA

BRIEF FOR THE UNITED STATES

Jeffrey H. Sloman
Acting United States Attorney
Attorney for Appellee
99 N.E. 4th Street
Miami, Florida 33132-2111
(305) 961-9130

Anne R. Schultz
Chief, Appellate Division

Lisa Tobin Rubio
Assistant United States Attorney

Kathleen M. Salyer
Assistant United States Attorney

Of Counsel

United States v. Beckett, Case No. 09-10579-BB

Certificate of Interested Persons

Undersigned counsel for the United States of America hereby certifies that the following is a complete list of persons and entities who have an interest in the outcome of this case who were not included in the Certificate of Interested Persons set forth in appellant's brief:

Acosta, R. Alexander

Rubio, Lisa Tobin

Salyer, Kathleen M.

Schultz, Anne R.

Sloman, Jeffrey H.

Kathleen M. Salyer
Assistant United States Attorney

Statement Regarding Oral Argument

The United States of America respectfully suggests that the facts and legal arguments are adequately presented in the briefs and record before this Court and that the decisional process would not be significantly aided by oral argument.

Table of Contents

Page:

Table of Contents

(continued)

Page:

Table of Contents

(continued)

Page:

Table of Citations

Table of Citations (Continued)

Cases: **Page:**

Statutes & Other Authorities:

Table of Citations (Continued)

Statement of Jurisdiction

The jurisdiction of this Court is invoked under 28 U.S.C. § 1291.

Statement of the Issues

1. Whether the district court correctly denied Beckett's motion to suppress evidence colleted as a result of law enforcement's written requests to American OnLine (AOL), MySpace, Comcast, and Bell South as well as evidence seized during a search pursuant to a warrant of Beckett's property and computer.

2. Whether sufficient evidence supports Beckett's convictions of possession and production of child pornography and coercion of a minor.

Statement of the Case

1. Course of Proceedings and Dispositions in the Court Below

On March 20, 2008, a federal grand jury in the Southern District of Florida, returned a 20-count superseding indictment charging appellant Timothy Beckett, a/k/a "chelzzz420zzz," a/k/a "2*cute*for*school," a/k/a "yesurifnotcuter," with possession of child pornography on July 18, 2007, in violation of 18 U.S.C. § 2252A(a)(5)(B) (Count One); four counts of production of child pornography on or about July 9, 2007, in violation of 18 U.S.C. § 2251(a) (Counts Two through Five); four counts of production of child pornography on or about June 2, 2007, in violation of 18 U.S.C. § 2251(a) (Counts Six through Nine); six counts of production of child pornography on or about June 21, 2007, in violation of 18 U.S.C. § 2251(a) (Counts Ten through Fifteen); four counts of coercion of a minor on various dates in June and July, 2007, in violation of 18 U.S.C. § 2422(b) (Counts Sixteen through Nineteen); and

distribution of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2) and (b)(1) (Count Twenty) (DE 34).

Beckett filed motions to suppress evidence that law enforcement had obtained pursuant to written requests to various on-line service providers as well as evidence discovered on computers that were seized during a search of Beckett's residence pursuant to a warrant (DE 42, 43). A magistrate judge issued a report recommending that the motions to suppress be denied (DE 56). After Beckett filed written objections (DE 57), the district court adopted the report and recommendation and denied the motions to suppress (DE 58). The case proceeded to trial. The United States dismissed Count Twenty at the close of the government's case (DE109:307), and a jury returned a verdict finding Beckett guilty as to the remaining counts (DE 73).

The district court sentenced Beckett to 180 months' imprisonment, to be followed by a life term of supervised release, and assessed him $1,900 (DE 91). Beckett filed a timely notice of appeal (DE 92). He remains incarcerated.

2. Statement of the Facts

A. The Offense Conduct

i. Introduction

In the summer of 2007, appellant Beckett created a MySpace[1] account using the profile of a 17-year-old female named "Chelsea." He contacted at least four underage young men on MySpace and continued communications with them through an America OnLine Instant Message (AIM) account under the name "yesurifnotcuter."[2] Beckett sent each of the young men nude photographs of a 17-year-old young woman, purporting that they were photographs of the sender. Each of the young men sent nude photographs of himself to Beckett in return. After Beckett had received the nude photographs from the young men, he replied to each with an instant message that revealed that he was actually a 21-year old male. Beckett threatened to distribute the nude photographs each of the young men had sent

---

[1] MySpace is a social network (DE108:91). A MySpace profile is an individualized web page that a user can customize to his liking (DE108:86). Each member of MySpace is assigned a unique "friend" identification number (DE108:87-88). These numbers cannot be changed (*id.*). In addition to the "friend" identification number, each MySpace user has a display name that can be customized to fit the user's profile (*id.*).

[2] An AOL instant message (AIM) is an instant message between two computers, without the use of a mailbox (DE108:77). Each AIM user has an unique screen name that the user has set up himself (DE108:78).

to their "friends" on their respective MySpace pages if they did not meet Beckett and permit him to perform oral sex on them. The facts relevant to each of the young men's internet encounters with Beckett and the investigation by law enforcement that ensued are as follows:

ii. JH (Counts Two - Five and Count Sixteen)

In the summer of 2007, when JH was 17 years old, he had a MySpace page under the display name "jonjonhasthevaccinetosenioritis"; the profile on that page included the fact that JH was in high school (DE 109:186, 207). JH received a random message on his MySpace page from someone he believed was a 17-year old girl (DE109:187-88, 195, 212; GX6.106; GX6.107-6.114). The individual who contacted JH had a MySpace friend identification that corresponded to the name "Chelsea Grammar" (DE108:98). JH and the individual exchanged AIM screen names and continued their communication on AIM (DE109:190). The individual who had contacted JH was Timothy Beckett, a 21-year old male who was posing as a teenage female and using the unique screen name "yesurifnotcuter" on AIM (DE108:78; DE109:190).

After some initial correspondence, in which Beckett asked JH some questions about himself, Beckett suggested that they exchange photographs of themselves (DE109:193-94). Beckett sent JH several photographs of a young woman, including

some that showed the young woman in the nude (DE109:194-95; GX4.101-4.114). JH then took nude photographs of himself and sent five photos to Beckett through AIM (DE109:195-96, 208-09; GX4:306-4.310; *See* DE108:130-31, describing these photographs as "male exposing genitals"). These photographs were later discovered on a computer seized from Beckett's bedroom pursuant to a warrant in a folder named "Jordan 2" and on JH's computer as well (DE108:134).

JH and Beckett continued their AIM chat and Beckett asked JH to meet him and permit him to give JH oral sex (DE109:198). Beckett offered, "I could come there or I could give you gas money" (DE109:198). When JH refused, Beckett replied that he had "something that will make you change your mind" and then sent the following message, in which he revealed that he was a 21-year-old male and threatened to send the nude photographs of JH to his friends on MySpace if JH did not accede to Beckett's demands:

> Okay. First off I'm going – I'm sorry to do this to you, but I'm really horny and I want to give you head. So here's what's going to happen. I'm going to throw you some cash, and you're going to let me suck you off, and you don't have to do anything at all to me, just chill and get head, and then you will never see or hear from me again.
>
> Reason I'm saying all this is 'cause I['m] really a guy. Good news, though. I'm not like some old fat guy like you're thinking. I'm your age, LOL. And, yeah, what can you do LOL.

> So, anyways, again, I'm sorry that I messed with you, but I always wanted to give a straight guy head, and this is the only way I can imagine it working. So let me do it, or I'm gonna have to send your picks to all your friends on MySpace, starting with your top list and comments.
>
> And don't bother making your page private, because I already have it pulled up. So I know it's weird for you, trust me, but I've already seen your cock. So just let me do it, get it over with, you get some cash, never see me again, and no one finds out. or I have to send them to everyone. If you sign off, then I start sending.

(DE109:198-99).

JH felt panicked (DE109:199). JH continued to refuse Beckett's demands and begged Beckett not to distribute the nude photograph of himself that he had sent to Beckett (DE109:200-02). JH even offered Beckett as much as $400-$500 if he would reconsider (DE109:202-04, 208). It was apparent to JH that Beckett had access to JH's friends on JH's MySpace page (DE109:204). Beckett demanded a meeting with JH in 20 minutes, stating "just do it so I don't have to ruin your life" (*id.*). At one point, Beckett became angry and sent a nude image of JH; Beckett insisted he would send the image to all of JH's friends on MySpace if JH did not meet Beckett immediately for sex (*id.*). JH notified the authorities.

iii. CL (Counts Six - Nine and Seventeen)

CL, who used the screen name "xmanofsteel1027," was 16 years old when Beckett, using the AIM screen name "yesurifnotcuter" and identifying himself as Chelsea or "Chelz," sent CL a "friend request" online (DE109:246, 248-49). From the profile that accompanied the request, CL understood that Chelsea was a 17-year-old girl who lived in the Wellington area of West Palm Beach (DE109:249; GX6.106). CL's internet profile showed that he was 16 years old (DE109:245-46, 258). CL and Beckett engaged in conversation over the internet; Beckett asked CL if he could go out (DE109:251; GX7.1).

Beckett sent photographs of a young woman, including some nude photographs, to CL (DE109:154, 265; GX7.102, 7.103, 7.104, 7.105, 7.106). CL sent nude photographs of himself to Beckett (GX4.3, 4.301; GX7.107, 7.108; *see* DE108:130-31, describing the photographs as depicting "male exposing genitals"[3]). After Beckett asked CL to go out with him (GX7.1 "If you cant get out tonight =(") and arranged to pick up CL at his house, CL gave Beckett his home address and phone number. CL explained that he had his mother's permission to go

---

[3] These photographs, which were on both Beckett's computer and CL's, were discovered in a laptop computer that was seized from Beckett's bedroom, under the user name "Timmy," in a desktop folder entitled "mike web cam" (DE108:132; DE109:155-52).

out, provided that he was picked up by 9:30 p.m. (DE109:252-53). There was a continuing exchange of messages concerning whether Beckett would reach CL's house by 9:30 and whether CL would be permitted to leave if Beckett did not arrive by that time (DE109:252-53; GX7.1). Beckett tried unsuccessfully to convince CL to sneak out of his house before 9:30 (DE109:254; GX 7.1). CL replied that he would not sneak out and Beckett replied with the same threatening message he had sent to JH, revealing for the first time the he was a 21-year-old male and threatening to disseminate nude photographs that CL had sent to him over the internet if CL would not meet Beckett and permit Beckett to perform oral sex (DE109:255-58; GX 7.1).

CL was scared and surprised (DE109:255). The chat continued, and CL expressed rage at having been duped by Beckett (DE109: 257, GX 7.1). CL continued to refuse to meet Beckett; CL told Beckett that it was too late in the evening for Beckett to pick him up and he would not disobey his mother by sneaking out of the house (DE109:257 "I'll not disobey her. Never have. Never will"). Beckett began to list the names of CL's friends on his MySpace page, and CL became afraid that Beckett would, in fact, broadcast the nude photographs of CL to his friends (DE109:260-61; GX 7.1).

Ultimately, CL informed his parents, they contacted the Boynton Beach Police Department and Det. Athol began to investigate (DE109:259). Det. Athol read the

AIM chats on CL's home computer and concluded that CL was being solicited for a violation of the Florida sexual battery statute (DE108:51). From his observation of the ongoing chat, Det. Athol concluded that it was "obvious" that the person who was communicating with CL online knew a "disturbing amount of information about him" (DE108:53).

Under the direction of Det. Athol, CL continued his online chat with Beckett and attempted to arrange a meeting site (DE109:259-63). Ultimately, the police were unable to find a suitable decoy to meet with Beckett and abandoned their attempt to set up a meeting with Beckett (DE109:265). CL terminated his online chat with Beckett; Beckett later called CL from a telephone on which the caller ID was blocked and left a voice mail message (DE109:59-60; GX7.111). When Det. Athol met with Beckett following Beckett's arrest, Det. Athol immediately recognized Beckett's voice as the voice on the recorded message (DE108:59). Beckett had revealed to CL that he had a "sidekick" phone as well as a Nokia music phone; CL had received calls from Beckett on the house phone as well as on his personal cellular phone (DE109:264; GX7.111). CL testified that if Beckett had identified himself as an adult male at the outset of their communications, CL would not have send nude photographs of himself to Beckett, nor would he have arranged to meet him (DE109:271).

iv. CH (Counts Ten - Fifteen and Eighteen)

CH, whose AIM screen name was "kooll1," was contacted on MySpace by Beckett, who was posing as "Chelsea" and using friend ID "Chelsea Grammar" (DE108:100). Beckett and CH began chatting on AIM, where Beckett used the screen name "yesurifnotcuter" (DE109:273; GX 4.311). CH was 16 years old at the time and believed that "Chelsea" was a 17- or 18-year old female (DE109:274-75; GX6.106). Initially, CH and Beckett exchanged messages once or twice a week for about a month (DE109:275). At some point in the conversation, CH revealed to Beckett that he was 17 years old (DE109:180: GX4.311).

Beckett asked to meet CH and suggested that they "trade some pics first"[4] (DE109:274-75; GX4.311). CH replied that he did not have any way of photographing himself (DE109:279-80, GX 4.311). Beckett replied, "don't u have a camera cell phone?" (GX4.311). When CH explained that he had recently lost his phone, Beckett responded "no webcam nothing =(something!!! lol" (GX 4.311). Beckett, as "Chelsea" agreed to send photos "but u can send back" and qualified that CH should send the photos in return "so I can pick u up" "and have some fun" (GX4.311). CH eventually took five photographs of himself in the nude using an old

[4] The log of CH's online chat with Beckett was located on the laptop seized from Beckett's bedroom pursuant to a warrant (DE109:143).

cellular phone and sent them to Beckett via AIM (DE109:286-87; GX 4.301, 4.302, 4.303, 4.304, 4.305; *see* DE108:130-31, describing the photos as "male exposing genitals").[5] Beckett, still posing as "Chelsea," then suggested that Chelsea's brother "Trent" could pick up CH and drive him to Chelsea's home so that Chelsea could perform oral sex on him (DE109:280-82). CH gave Beckett his home address (DE109:281-82).

Beckett picked up CH at his house, posing as the brother of the young woman with whom CH had corresponded online (DE109:282-83). Beckett drove to a WalMart where he cashed his paycheck (DE109:283). As he drove away, Beckett showed CH the cash and offered to pay CH to take off his clothes (DE109:283). CH was hesitant at first, but eventually allowed Beckett to pay him to take off his shirt and then to display his genitals (DE109:285). Beckett continually urged CH to drink from a bottle of liquor that Beckett had in the car, but CH refused (DE109:284). CH felt "scared" and "terrified," and insisted that Beckett drive him home (DE109:285).

At that point, Beckett's car was stopped by the police (DE109:285). The police officer discovered that Beckett's driver license had been suspended and requested that CH drive the car (DE109:286). CH drove himself home (*id.*). After CH returned

---

[5] These photos were in the laptop seized from Beckett's bedroom pursuant to a warrant, under the user name "Timmy" in a folder on the desktop named "cool1" (DE108:132).

home, he received additional AIM communications from Beckett, who threatened that if CH would not met with him, Beckett would send the nude photographs of CH to his friends and tell them that CH was "gay" (DE109:287).

CH testified that he would not have sent photographs to Beckett or agreed to meet with him if he had known that Beckett was an adult male (DE109:287). CH identified Beckett in court as the person who had picked him up and driven him around (DE109:285).

v. MG (Count Nineteen)

In June 2007, when he was 16 years old, MG, who used the AIM screen name "pmpnmotion," was contacted by Beckett, using the name "Chelsea" and the AIM screen name "yesurifnotcuter" (DE109:217, 220-21; GX6.106). MG began an internet chat with Beckett and they exchanged addresses for their respective MySpace pages (DE109:219-21; GX4.4, 4.401-4.403). The logs of their online chat were discovered in Beckett's laptop computer (DE109:143). At some point in the conversation, MG revealed to Beckett that he was 16 years old (DE109:226, 243). Beckett was posing as a 17-year-old girl named Chelsea, and represented that he was not looking for a boyfriend, just a "hot guy to play around with " (DE109:225, 227). Beckett asked MG the size of his genitals and if he liked oral sex and then suggested that they exchange photographs (DE109:225-27; GX4.400, 4.401, 4.402). Beckett

sent MG two nude photographs of a young woman; at Beckett's suggestion, MG then send an MSN live feed of himself in the nude to Beckett (DE109:228-30). After Beckett had received the live feed of the nude MG, he sent MG essentially the same threatening message he had sent to JH, CL and CH (DE109:230-31; GX10.102).

MG initially thought that Beckett's response was a joke, but he quickly realized that it was not (DE109:232-34). MG was very concerned because it was clear to him that Beckett had a list of the friends on MG's MySpace page (DE109:235-36; GX8.109-8.112). Beckett continued to send instant messages, and the tone of those messages became increasingly aggressive (DE109:232). Beckett insisted that MG meet him and permit him to perform oral sex and also threatened to distribute the nude photographs of MG to the friends on MG's MySpace page if MG refused to meet with him (DE109:233-36). MG knew that Beckett had the list of all the friends on MG's MySpace page (DE109:236).

MG revealed to Beckett that he had recorded Beckett's IP address and that MG's mother had a friend who was an attorney who would use that information as evidence against Beckett (DE109:236-37). MG also claimed that the photos he had sent were of someone else, not MG, hoping that Beckett would lose interest in sending them (DE109:187). At that point, it appeared to MG that Beckett was attempting to send back to MG the live feed of MG in the nude that MG previously

had sent to Beckett (DE109:238). Beckett disconnected from the AIM chat session and MG never heard from him again (DE109:238). MC testified that he would not have consented to meeting with Beckett if he had known Beckett was a man (DE109:233).

vi. The Investigation

JH had contacted the National Center for Missing and Exploited Children (NCMEC) and reported that an adult had solicited him over the internet for sex. On July 10, 2007, the NCMEC contacted Det. Toby Athol of the Boynton Beach, Florida, Police Department who, in turn, forwarded the information to the Palm Beach Sheriff's Office (DE108:46-48). That office began an investigation of the internet solicitation (*id.*). Palm Beach Sheriff's Deputy Cass Collins obtained the laptop that JH had used to communicate with Beckett under his screen name "yesurifnotcuter." CL's parents contacted the Boynton Beach Police Department, and Det. Athol was assigned to that case (DE108:53?). Det. Athol immediately noticed that the originating screen name for the AIM chat with CL was the same as the originating screen name for the AIM chats that Det. Athol had referred to the Palm Beach County Sheriff's Office the previous day (DE108:53).

During the investigation, Det. Athol and Det. Collins sent AOL a request for information relating to the screen name "yesurifnotcuter" (DE108:78). AOL

provided the information it had concerning that screen name and the connection logs associated with it, including the internet protocol (IP) address (DE108:81-82; GX10). The IP address belonged to Comcast Communications, another service provider (DE108:83). The detectives also requested information from MySpace.com (DE108:86). MySpace provided subscription information (DE108:87-91; GX8.1; 8.102- 8.106; 8.116-8.126; GX8-CDROM-1). The information provided by AOL and MySpace in response to the detectives' requests enabled law enforcement to establish connections between Beckett and two of the victims, JH and CL. Using Beckett's unique "friend" identification number for his MySpace account under the name "Chelsea Grammar," the forensic examiner was able to find exchanges of messages between Beckett and JH and between Beckett and CH on their respective MySpace pages (DE108:98-100; GX 8.104 (CH); GX8.105 (MG); GX8.106 (CL); GX8.108 (JH)).

Det. Athol also sent an "exigent circumstances" letter to BellSouth's subpoena compliance department and requested the source of the blocked telephone call to CL (DE 108:57-61). Det. Athol learned that the call to CL's telephone had originated from a T-Mobile phone (DE108:62). T-Mobile provided Det. Athol with a live GPS tracking of the phone (DE108:62). Det. Athol was able to track the phone to a

residence in the Wellington area of West Palm Beach, which enabled the detectives to identify Beckett as the suspect (DE108:63-64).

The detectives obtained a warrant to search Beckett's residence; they took Beckett into custody when they arrived to conduct the search (DE108:64). The ensuing search of Beckett's bedroom yielded computers and computer related media, including a Dell Inspiron B130 laptop, a Dell Dimension 4550 tower (DE108:110), and a Samsung 60-gigabyte hard drive (DE108:112; DE109:166). Det. Patrick Paige of the Palm Beach County Sheriff's Office Computer Crimes Unit, who testified as an expert in computer forensics, examined the computers seized from Beckett's bedroom and provided further evidence of the internet communications between Beckett and the juvenile victims (DE109:166). In the laptop computer, Det. Paige found evidence of AIM chat sessions with CH ("kooll1") (GX4.311); MG ("pmpnmotion") (GX4.4, 4.401, 4.402, 4.403), and CL ("xmanofsteel"). In a temporary internet file on JH's computer, Det. Paige discovered a MySpace page for the screen name of "chelzzz420zzz," a screen name associated with Beckett (DE 109:146; GX6.106). He found the same page on Beckett's computer (*id.*; GX6.106.1). He also found chats on JH's computer under another of Beckett's monikers, "yesurifnotcuter" (DE109:147). Det. Paige also located chat sessions and images on CL's hard drive (DE109:153). Those images were the same as those he

had found on Beckett's computer (DE109:156). In addition, Det. Paige found approximately 23 movies of suspected child pornography on the laptop and approximately 43 such videos on the computer tower (DE 108:118). Some of the pornographic videos were located under the user name "Timmy" in a folder on the desktop named "porn" (DE109:165).

An expert testified that the images depicted real people, some of whom were sexually mature adults and others who were prepubescent children (DE109:178). At least some of the videos showed sexual acts between mature adults and prepubescent children and others between older children and prepubescent children, all of which were of a sadomasochistic nature (DE109:178-79). He also examined victims' computers for images of child pornography (DE108:124-25; GX 6 CD-ROM 1; GX 7 CD-ROM 1).

All communications through AOL are transcribed through AOL's headquarters in Northern Virginia (DE108:74). The parties stipulated to the admission of a declaration of Tamara McBride, the online services custodian of records for Microsoft Corporation, which stated that Microsoft operated the web-based Windows Live Hotmail and e-mail and Windows Live Messenger Services, and none of the servers supporting those services are located in the state of Florida (DE109:297). The parties also stipulated to the admission of a letter from Comcast Corporation that

pertained to the IP address associated with the AIM screen name "yesurifnotcuter" (DE 109:298; *see* DE108:82). The letter provided the subscriber name, home address, and telephone number associated with that Comcast account (DE 109:298).

After he was arrested and given his *Miranda*[6] warnings, Beckett admitted that he had communicated with several male juveniles on MySpace and AOL/AIM using the identity of a 17-year old female (GX1; GX2). Beckett confessed that he had used extortion and blackmail once the juveniles found out that he was a man instead of a woman (*id.*). Beckett admitted that he had more than 100 images of child pornography and more than 30 movies that contained child pornography on his computer (DE108:47; GX1; GX2).

B. Facts Pertaining to Beckett's Motion to Suppress Evidence

i. The Motions to Suppress Evidence and the Government's Response

Beckett filed a motion to suppress "any and all evidence collected, seized, and developed as a result of written requests by law enforcement to America OnLine (AOL), MySpace, Comcast and Bell South (DE 13). He argued that law enforcement had gathered evidence from these internet service providers (ISPs) before subpoenas for that information had been issued, in violation of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2703, which generally prohibits law enforcement

[6] *Miranda v. Arizona*, 346 U.S. 436, 88 S. Ct. 1602 (1966).

from obtaining subscriber information from an internet service provider without a valid search warrant, court order, or administrative or grand jury subpoena (*id.*). Beckett argued that the exception for exigent circumstances, which is set out in 18 U.S.C. § 2702, did not apply in this case (*id.*). He also argued that the fact that subpoenas ultimately were issued to the ISPs who furnished the information did not cure the alleged violation (*id.*).

Beckett also filed a motion to suppress the evidence that was seized during a search pursuant to a warrant of the residence where he was living (DE 14). Beckett argued that the warrant did not authorize a search of the information stored in the hard drives of the computers that were the subject of the warrant (*id.*). Thus, he claimed that the items collected were seized in violation of the Fourth Amendment.

The United States responded that there was no violation of the ECPA in this case (DE 22). The United States relied on an exception to the requirement of an administrative, grand jury, or trial subpoena, set out in §§ 2702(c)(4) and (5), which permits disclosure of a record or other information pertaining to a subscriber to a governmental entity if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency (*id.*). The United States also argued that the subscriber agreements with the internet service providers specifically

prohibited obscene or pornographic messages or images and Beckett, as a subscriber, was on notice that he had waived any privacy interest he had in his internet communications by his flagrant violations of the terms and conditions of the subscriber agreements (*id.*). The United States attached copies of the subscriber agreements to its response.

ii. The Hearing before the Magistrate Judge

A magistrate judge conducted a hearing on the motion (DE31). Det. Collins testified that she became involved in the investigation in this case after she was notified by the NCMEC that an juvenile in Palm Beach County had reported that someone on the internet was pretending to be a female and was luring this juvenile to engage in sexual conduct (*id.* at 10-11). The following day, Det. Collins received information concerning a juvenile in Boynton Beach, Florida, who also had encountered an individual on the internet who was pretending to be a female and was luring that juvenile to engage in sexual conduct (*id.* at 11-12). Det. Collins suspected that both juveniles had corresponded with the same individual on the internet because there was one paragraph in each of their chat sessions that was identical (*id.* at 12).

Det. Collins's investigation revealed that an individual purporting to be a 17-year-old female had met the victim known as JH on MySpace (*id.* at 17). This individual sent a nude photograph of a young woman over the internet to JH and

requested that JH send a nude photograph of himself (*id.* at 15-16). JH took a nude photograph of himself with his camera phone and sent it to the person purporting to be a 17-year-old girl (*id.*). At that point, the sender revealed to JH that he was really a man and stated that he wanted to engaged in oral sex with JH (*id.* at 13-16). The sender threatened that he would "send your pics to all your friends on MySpace, starting with your top list and comments" if JH would not engage in oral sex with him (*id.* at 14-16). JH contacted NCMEC, and that agency contacted Det. Collins (*id.* at 16). NCMEC furnished Det. Collins with the victim's name and the screen name of the individual who had sent the threatening message (*id.* at 11). Det. Collins met with the victim and reviewed a series of online chats between the victim and the sender (*id.* at 11). When she met with him, JH told Det. Collins that he believed that the sender was an adult male (*id.* at 62).

CL, a 16-year-old young man from Boynton Beach, Florida, engaged in similar correspondence with and sent a nude photograph of himself to someone he thought was a 17-year-old girl (*id.* at 18-20). At some point in the correspondence, CL had actually revealed his home address to the sender (*id.* at 19). After the sender revealed to CL that he was a man and threatened to broadcast the nude photographs of the CL if CL did not engage in oral sex with the sender, CL contacted the Boynton Beach

Police Department while he continued to chat online (*id.* at 15, 19).[7] Det. Toby Athol of the Boynton Beach Police Department met with CL and instructed CL on what to say in his continuing internet communications with the perpetrator (*id.* at 19). At one

---

[7] The contents of the communications from the sender to both JH and CL, which were identical, were as follows:

> Okay. First off I'm going – I'm sorry to do this to you, but I'm really horny and I want to give you head. So here's what's going to happen. I'm going to throw you some cash, and you're going to let me suck you off, and you don't have to do anything at all to me, just chill and get head, and then you will never see or hear from me again.
>
> Reason I'm saying all this is 'cause I['m] really a guy. Good news, though. I'm not like some old fat guy like you're thinking. I'm your age, LOL. And, yeah, what can you do LOL.
>
> So, anyways, again, I'm sorry that I messed with you, but I always wanted to give a straight guy head, and this is the only way I can imagine it working. So let me do it, or I'm gonna have to send your picks to all your friends on MySpace, starting with your top list and comments.
>
> And don't bother making your page private, because I already have it pulled up. So I know it's weird for you, trust me, but I've already seen your cock. So just let me do it, get it over with, you get some cash, never see me again, and no one finds out. or I have to send them to everyone. If you sign off, then I start sending.

(DE at 13-14).

point, the perpetrator had contacted CL by telephone, although he had blocked the sender information for the call (*id.* at 30).

Because of the similarity in JH's and CL's internet chat sessions, Det. Collins concluded that both were corresponding with the same individual on the internet (*id.* at 21-22). Det. Collins was concerned because she knew that the perpetrator had nude photographs of both JH and CL and had threatened to distribute them over the internet; moreover, he had the home addresses for both victims and the telephone number for one of them (*id.* at 21-22). She concluded that it was possible that the perpetrator had similar threatening communications with other juveniles and that any of them could be threatened or harmed (*id.* at 21-22).

Det. Collins did not have the authority to issue an administrative subpoena, and she was unable to reach the Assistant State Attorney who had the authority to issue subpoenas in such cases (*id.* at 21). As a result, Det. Collins sent letters to AOL and to MySpace requesting subscriber information and IP information linked to the sender of the threatening correspondence to JH (*id.* at 22-24; GX 3 (AOL); GX 2 (MySpace)). Det. Collins requested the information on the basis of an imminent threat (*id.* at 25). Det. Athol sent similar correspondence to T-Mobile, AT&T and Bell-South to determine the source of the threatening messages to CL and the telephone number from which the perpetrator had called CL (*id.* at 28-30).

MySpace and AOL furnished Det. Collins with the requested subscriber information and logs (*id.* at 25). The providers did not divulge the contents of any communications that were associated with the designated screen names (*id.* at 24-25). Det. Collins learned that Comcast Communications owned the AOL and MySpace IP addresses (*id.* at 26). Det. Collins obtained the subscriber information associated with that IP address by filing an emergency situation disclosure request with Comcast (*id.* at 26-28). The subscriber information was linked to a residence in West Palm Beach, Florida (*id.* at 27, 36). Based on information from Bell South and T-Mobile, detectives were able to determine who had telephoned the victim in Boynton Beach (*id.* at 39). Det. Collins and Det. Athol obtained a warrant to search the premises linked to the Comcast subscriber information (*id.* at 39; GX 11).

The internet subscriber agreements for Comcast Communications, MySpace, AOL, and T-Mobile specifically prohibit users from transmitting indecent or pornographic material or from sending harassing or threatening communications (*id.* at 32-36). The agreements also provide that the ISPs reserve the right to cooperate with law enforcement or to take legal action to prevent violations of the terms and conditions of the agreement (*id.* at 32-35).

Following the presentation of evidence, the magistrate judge entertained argument on the motions (*id.* at 68). The government argued that suppression of the

evidence was not a remedy for violation of § 2703; the remedy was civil damages (*id.* at 70-71). The government also argued that there was no violation of § 2703 (*id.* at 73). The statute authorized ISPs to disclose information to law enforcement where they have a good faith belief that the information will be used in law enforcement (*id.*).

iii. The Magistrate Judge's Report and Recommendation

The magistrate judge issued a report recommending that the motions to suppress be denied (DE 28). As to the motion to suppress information that law enforcement had obtained in response to its "exigent circumstance" letters to the ISPs, the magistrate judge found that there was no Fourth Amendment protection of the subscriber information (*id.* at 6). The terms and conditions of the subscriber agreements with the internet and phone service providers contained clauses that prohibited subscribers from posting or transmitting child pornography, stalking, and harassment, and reserved to the ISPs the right to investigate, take legal action, and cooperate with law enforcement (*id.* at 3). These contracts had terms and conditions that permitted the ISPs to turn over information in limited circumstances (*id.*). Moreover the remedy for a violation of ECPA is a civil action in damages, not suppression of evidence in a criminal proceeding (*id.*).

As to Beckett's claim that the officers had exceeded the scope of the warrant when they searched the computer hard drives for pornographic images, the magistrate judge concluded that the challenged evidence was otherwise described in the warrant application and incorporated by reference into the warrant and, therefore, was properly the subject of the search (*id.* at 10). The agents' affidavit, which was incorporated by reference in the search warrant, described the forensic computer examination process utilized during a computer search, including the process of searching through all the files on the computer (*id.*). The magistrate judge found that the process of searching the specific computer files was "functionally described" in the search warrant and the search did not exceed the scope of the warrant (*id.* at 11).

iv. The Objections to the Report and Recommendation and Response

Beckett filed written objections to the report and recommendation (DE 30). He argued that, notwithstanding the terms and conditions of the service agreements with the ISPs, he had a reasonable expectation of privacy in using the internet services and the records of his internet service use should not have been released without a warrant or court order (*id.*). Beckett further argued that there were no exigent circumstances in this case that permitted the release of the records without a court order or subpoena (*id.*). Beckett also disagreed with the magistrate judge's conclusion that there are only civil remedies available for violations of § 2703 (*id.*). Beckett maintained that

the search warrant did not provide for the search of computer files or the information stored in the computers and devices (*id.*). Thus, he concluded that the contents of his computer files had been seized in violation of his Fourth Amendment rights (*id.*).

In response, the United States argued that Beckett did not have a reasonable expectation of privacy in the internet communications at issue and that the agents did not exceed the scope of the search warrant (DE 32). The search was specifically limited to the scope of the warrant, to items related to the investigation of child pornography and child exploitation (*id.*).

v. The District Court's Order

Following a *de novo* review of the record, the district court affirmed and adopted the magistrate judge's report and recommendation and denied the motions to suppress information furnished by the ISPs and information seized during the search of Beckett's computers (DE 33).

3. Standards of Review

A ruling on a motion to suppress presents "a mixed question of law and fact." *United States v. Steed*, 548 F.3d 961, 966 (11th Cir. 2008) (quoting *United States v. Boyce*, 351 F.3d 1102, 1105 (11th Cir. 2003)). This Court accepts the district court's factual findings unless they are clearly erroneous, construing all facts in the light most

favorable to the prevailing party below. *Id.* The district court's application of the law to the facts is reviewed *de novo*. *Id.*

Whether the record contains sufficient evidence to support a jury's guilty verdict is question of law that this Court reviews *de novo*. On review of a guilty verdict, evidence is viewed in a light most favorable to the government, with all reasonable inferences and credibility choices made in the government's favor. *United States v. Calderon*, 127 F.3d 1314, 1324 (11th Cir. 1997).

Summary of the Argument

The district court did not err in denying Beckett's motion to suppress information that law enforcement obtained from ISPs pursuant to "exigent circumstance" letters, which identified the IP for the AOL user name and MySpace friend identification for the individual who had sent threatening messages to two juveniles, and identified the blocked T-Mobile telephone number from which the sender of the threatening messages had telephoned one of the juveniles. The request for information was related to a legitimate investigation by law enforcement, and the officers had a good faith basis to believe that the two juvenile victims may be in harm's way, in light of the fact that the perpetrator had their home addresses and the phone number for one of the victims.

The district court did not err in denying Beckett's motion to suppress evidence taken from the computer that was seized from Beckett's bedroom during a search pursuant to a warrant. The search warrant, which incorporated by reference the law enforcement officers' affidavits in support of the warrant, authorized the search of the computer hard drives, and the resulting search did not exceed the scope of the warrant.

Sufficient evidence supports Beckett's convictions of possession of child pornography, production of child pornography and coercion of a minor.

– The evidence that Beckett organized numerous videos of child pornography on his computer in a file marked "porn"; that he solicited nude photographs from young men he knew were under the age of 18 and then stored those photographs on his computer; and that Beckett even acknowledged to one of the victims that the photographs the victim had sent to Beckett were "porn" sufficiently establishes Beckett's knowing possession of child pornography, as charged in Count One.

– The evidence that Beckett convinced four juveniles to take nude photographs of themselves and to transmit those photographs to Beckett via AIM or an MSN feed sufficiently supports Beckett's convictions of production of child pornography, as charged in Counts Two through Fifteen.

– The evidence that Beckett threatened to broadcast the nude photographs of his victims to the victims' friends on their MySpace pages if the victims did not meet Beckett and permit him to perform oral sex upon them (a violation of the Florida sexual battery statute), supports Beckett's convictions of coercion of a minor, as charged in Counts Sixteen through Nineteen.

Argument

I. The District Court Correctly Denied Beckett's Motions to Suppress Evidence.

Beckett challenges the district court's denial of his motion to suppress evidence of the information law enforcement obtained from the ISPs that ultimately led law enforcement to him as well as the evidence obtained from the computers that were seized pursuant to a warrant. Neither of his claims has merit.

A. Evidence Obtained from ISPs

Beckett contends that the district court erred in denying his motion to suppress the information that law enforcement officers obtained from the ISPs through the use of "exigent circumstance" letters (Br. at 12-16). He argues that law enforcement acted in violation of the ECPA, 18 U.S.C. § 2701 *et seq.*, which generally requires that law enforcement obtain a valid search warrant, court order, or subpoena in order to obtain subscriber information from an ISP. 18 U.S.C. § 2703(c). His argument

appears to be based on the assumption that the exception to the requirement of a warrant, court order or subpoena, which applies in emergency circumstances, did not apply here (*see* Br. at 14). He argues that Det. Collins misrepresented in her requests to the ISPs the information that allowed the ISPs to release information without a warrant or court order (Br. at 16). The record does not support Beckett's claims.

First, there was no violation of the ECPA. Section 2703(c) governs the disclosure by ISPs to governmental entities of records concerning electronic communication service or remote computing service. That section provides as follows:

> **(C) Records concerning electronic communication service or remote computing service** - (1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber or to a customer of such service (not including the contents of communication) only when the governmental entity –
>
> **(A)** obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;
>
> **(B)** obtains a court order for such disclosure under subsection (c) of this section;
>
> **(C)** has the consent of the subscriber or customer to such disclosure;

> **(D)** submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer or such provider, which subscriber or customer is engaged in telemarketing (as that term is defined in section 2325 of this title); or
>
> **(E)** seeks information under paragraph (2).

18 U.S.C. § 2703(c)(1). Paragraph (2), in turn, provides:

> **(2)** A provider of electronic communication service or remote computing service shall disclose to a governmental agency, the –
>
> **(A)** name;
>
> **(B)** address;
>
> **(C)** local and long distance telephone connection records, or records of session times and duration;
>
> **(D)** length of service (including start date) and type of service utilized;
>
> **(E)** telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
>
> **(F)** means and source of payment for such service (including any credit card or bank account number),
>
> of a subscriber to or a customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

18 U.S.C. § 2703(c)(2).

Section 2702(c) provides an exception to the requirement of a warrant or administrative subpoena in certain circumstances. As relevant to this case, that section authorizes disclosure:

> (4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency.

18 U.S.C. § 2702(c)(4).

In this case, the information that the detectives sought from the providers fell within the exception in § 2702(c)(4).[8] At the time that the letters were sent to AOL MySpace, T-Mobile and Bell-South, the detectives knew that there were two juvenile males who had communicated via the internet with an adult male who represented himself to be a 17-year-old girl; that the juvenile males had transmitted nude photographs of themselves to the adult male, thinking he was a teenage girl; that the adult male had attempted to force each of the juveniles to meet with him and to permit him to perform oral sex on them; that the adult male had threatened to broadcast the

---

[8] At this point, the officers had probable cause to believe that a crime had been committed and there were exigent circumstances that warranted their immediate demand for the records of the internet communications under traditional Fourth Amendment jurisprudence as well. *See United States v. Holloway*, 290 F.3d 1330, 1337 (11th Cir. 2002).

nude photographs of the juveniles over the internet if they did not comply with his demands; and that the adult male had the home addresses of both juveniles and the home telephone number for at least one of them and had called that number at least once (DE31 at 21-22). Moreover, in Det. Collins's view, it was entirely possible that the perpetrator had similar threatening communications with other juveniles and that any of them could be threatened or harmed (*id.* at 21-22). The tone of the e-mail communication lent a sense of urgency to the matter as well. In his e-mails to the juveniles, the sender made it clear that the juvenile's MySpace page was open, so it was too late for the juvenile to limit the sender's access to the page or to the friends listed on the page. He also suggested that the juveniles had no recourse against him if he sent out the photographs (GX7.1: " yeah, what can you do? LOL"). Thus, there was ample evidence to support a finding that there was an emergency involving the threat of serious physical injury that warranted immediate disclosure of the requested information.

Significantly, the detectives sought and received only subscriber information relating to the specified internet protocol addresses. They did not request that the service providers divulge the contents of any electronic communications and none were divulged (DE31 at 24-25). Subscriber information provided to an internet service provider is not protected by the Fourth Amendment's privacy expectation.

See United States v. Perrine, 518 F.3d 1196, 1204-05 (10th Cir. 2008) (collecting cases).

Finally, Section 2708 of the ECPA contains an "exclusivity of remedies" provision, which provides that "[t]he remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter." 18 U.S.C. § 2708. Section 2707 describes the remedies for violations of the Act as including civil actions for violators other than the United States and administrative discipline against federal employees in certain limited circumstances. *See* 18 U.S.C. § 2707. Thus, a violation of the ECPA does not warrant exclusion of the evidence.

B. Evidence Obtained During the Search of Beckett's Computers.

Beckett argues that the evidence seized from his home computer should have been suppressed because the officers' search exceeded the scope of the search warrant (Br. at 16-20). His claim has no merit. The search warrant (DE 14 at 18-20) and the 12-page affidavit in support of the search warrant (DE 14 at 6-19), which was incorporated into the search warrant (*see* DE 14 at 18), amply described the items to be searched to include the contents of the computers, hard drives, etc.

It is well settled that the language of a search warrant must describe the items to be seized with sufficient particularity; the language must be sufficiently definite

to enable the searcher to reasonably ascertain and identify the things authorized to be seized. *United States v. Khanani*, 502 F.3d 1281, 1289 (11th Cir. 2008). However, the particularity requirement of the Fourth Amendment must be applied with a practical margin of flexibility, taking into account the nature of the items to be seized and the complexity of the case under investigation. *See United States v. Wuagneux*, 683 F.2d 1343, 1349 (11th Cir. 1982).

The language of the search warrant, which incorporated by reference the detectives' affidavits, sufficiently demonstrates that the search warrant anticipated the search of the computer as well as the hard drives. The affidavit in support of the search warrant contained a section entitled "Specifics of Search and Seizure of Computer Systems" (*see* DE 14 at 8-9). That section explained that searches and seizures of evidence from computers commonly requires that law enforcement officers seize most or all computer items and cellular telephones/devices, including "hardware, software, and instructions" to be processed later by a qualified computer forensic expert in a controlled laboratory environment (*id.*). The affidavit explained that computer storage devices, such as "hard disks, diskettes, tape, removable drives" can store the equivalent of thousands of pages of information and that criminal evidence contained within those pages is often concealed by the manner in which it is stored. (*id.*). As a result, the searching process requires that "searching authorities

examine all stored data to determine whether it is included in the search warrant" (*id.*). The affidavit further explained that the search procedure was designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password protected, and/or encrypted files (*id.*). The affidavit concluded that in order to fully retrieve the data from the computer system, the forensic analyst would need "all magnetic storage devices, as well as the central processing unit" (*id.*). In this case, given the fact that the evidence consisted of graphic files, the computer's monitor and printer were "essential to show the nature and quality of the graphic images which the system could produce" (*id.*). Finally, the affidavit stated that there was probable cause to believe that "the computer and its storage devices, the monitor, keyboard, modem, printer, as well as all internal and external storage devices and cellular phones/PDA/Sidekicks, etc." were all instrumentalities of the crime under investigation (*id.* at 9).

The affidavit in support of the search warrant was equally explicit as to the "Property Sought" (*id.* at 10). From the affidavit, it was clear that law enforcement sought authorization to search for and seize "computers, personal computers, computer peripherals, modems, computer printers, floppy disk drives, hard disk drives, diskettes, tapes, computer printouts, computer software, computer programs and applications, computer manuals, system documentation" (*id.*). Significantly, the

affidavit in support of the search warrant contained an "Informational Glossary of Terms Applicable to the Affidavit" which provided detailed definitions of several terms used in the application, including "Hardware" and "Software" (*id.* at 15).

Moreover, Beckett's argument that the search in this case was unlawful because it was not "directed towards specific objects in it believed to be instrumentalities by which the crime charged was to have been committed" is unavailing. Det. Athol's statements in the affidavit in support of the warrant explained the reason for the apparently broad reach of the warrant. He explained that computer users who desire to conceal criminal evidence often store the information in random order with deceptive file names. In addition, they can create attributes that enable them to hide from view the directories and sub-directories that contain the criminal evidence (DE 14 at 8). As a result, the computer forensic examiner is often required to examine all data stored on a computer to determine whether or not it is within the scope of the search warrant (*id.*). There is no evidence that the ultimate search of the computer components was not as specifically directed as possible, however. The Tenth Circuit addressed this issued in *United States v. Burgess*, — F.3d —, 2009 WL 2436674 (10th Cir. Aug 11, 2009), and observed: "it is folly for a search warrant to attempt to structure the mechanics of a computer search and a

warrant imposing such limits would unduly restrict legitimate search objectives." *Id.*, slip op. at 12. The court continued:

> One would not ordinarily expect a warrant to search filing cabinets for evidence of drug activity to prospectively restrict the search to "file cabinets in the basement" or to file folders labeled "Meth Lab" or "Customers." And there is no reason to so limit computer searches.

Id. at 12-13.

Beckett's reliance on this Court's decision in *United States v. Mitchell*, 565 F.3d 1347 (11th Cir. 2009), is misplaced. In *Mitchell*, this Court reversed the district court's denial of a motion to suppress a search of a computer hard drive based on its determination that a 21-delay in obtaining a warrant to search the computer hard drive following its seizure from the owner's residence was not reasonable under the circumstances. *Id.* at 1352-53. In reaching that determination, this Court weighed the defendant's possessory interest in the computer against law enforcement's justification for the delay[9] in obtaining the search warrant and concluded that while the possessory interest was substantial, there was no compelling justification for the delay. *Id.* at 1351.

---

[9] The delay in obtaining the search warrant was attributed to the fact that the only law enforcement agent in the district who was qualified to conduct the forensic search of the computer hard drive for child pornography left for a two-week training session three days after the seizure of the hard drive and did not apply for a warrant to search it until he returned to the district (*id.* at 1351-52).

In this case, by contrast, the agents had a warrant to search Beckett's computer and hard drive when they arrived at his residence (DE108:64). There are no claims of unnecessary delay in securing a search warrant in this case and *Mitchell* is inapposite.

II. Sufficient Evidence Supports Beckett's Convictions.

Beckett challenges the sufficiency of the evidence to sustain his convictions of possession of child pornography, as charged in Count One (Br. at 21); production of child pornography, as charged in Counts Two through Fifteen (Br. at 22); and coercion of a minor, as charged in Counts Sixteen through Nineteen (Br. at 22). On review of a guilty verdict, this Court views the evidence in a light most favorable to the government, with all reasonable inferences and credibility choices made in the government's favor. *United States v. Calderon*, 127 F.3d 1314, 1324 (11th Cir. 1997). Viewed in that context, there was ample evidence to sustain Beckett's convictions.

A. Possession of Child Pornography on July 18, 2007, in Violation of 18 U.S.C. § 2252A(a)(5)(B) (Count One)

Beckett challenges the sufficiency of the evidence to support his conviction of possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). He does not dispute that the material found on his computer hard drive and other storage

devices was child pornography; he argues that there was not proof that he downloaded the material and actively stored it on the computer.

As the jury was instructed in this case, in order to prove a violation of 18 U.S.C. § 2252A(a)(5)(B), the government was required to prove (1) that Beckett knowingly possessed materials that contained child pornography on the date charged in the indictment; (2) that Beckett knew that the visual depictions were of a minor engaged in sexually explicit conduct; and (3) that the visual depictions had been mailed, shipped, or transported in interstate or foreign commerce by computer (DE110:371-72). The court's instructions to the jury defined "child pornography" as "any visual depiction, including any photograph, film, video, picture, or computer image or picture whether made or produced by electronic, mechanical, or other means of sexually explicit conduct where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct" (DE110:378). The court defined "sexually explicit conduct" to include actual or simulated sexual intercourse as well as lascivious exhibition of the genitals or pubic area of any person" (*id.* at 378-79). There was ample evidence from which a jury could have concluded that Beckett knew he was in possession of child pornography.

The government's computer forensic expert, Det. Patrick Paige, testified that there were three separate user names associated the laptop computer that was seized

from Timothy Beckett's bedroom – "Timmy," "Pizza Hut," and "Tim" (DE108:119). Det. Paige located 23 suspected child pornography videos on the laptop and an additional 43 videos of suspected child pornography on the tower computer that was seized from the same location (DE108:118). Some of the pornographic videos were located under the user name "Timmy" in a folder on the desktop named "porn" (DE109:165). These videos could only have been organized in that fashion on the desktop if the user had so organized them (*id.*). Given the nature of the contents and the title of the desktop folder in which they were organized, a reasonable jury could have concluded that Timothy Beckett had organized it there and was well aware that he was in possession of child pornography.

In the context of receipt of child pornography, in violation of 18 U.S.C. § 2252A(a)(2), courts have considered four factors to determine whether the defendant has knowingly received the pornography: (1) whether the images are found on the defendant's computer; (2) the number of images of child pornography found there; (3) whether the content of the images was evidence from their filed names; and (4) defendant's knowledge and ability to access the storage area for the images. *See United States v. Miller*, 527 F.3d 54, 67 (3d Cir. 2008) (collecting cases). These standards are equally probative of Beckett's knowing possession of child pornography in this case.

The evidence that Beckett had received nude photographs through AIM or MSN from each of his four victims, all of whom were under the age of 18 (DE109:195, 212 (JH); DE109:215 (MG); DE109:245 (CL); DE109:272 (CH)), also supports a finding that Beckett knowingly possessed child pornography. The three victims whose internet correspondence with Beckett forms the basis of Counts Two through Fifteen each sent nude photographs of themselves to Beckett via AIM or a live feed (DE109:194-95; 228-30; 286-87 GX4.101-4.114; GX4.301-4.305; GX4.306-4.310; GX7.107-7.108). Those nude images, which primarily showed young males exposing their genitalia (*see* DE108:130-31) constitute child pornography.

There is no question that Beckett understood that fact and was well aware that those images were on his computer. Beckett obtained these images by sending AIM messages to each of his victims and enticing them to send him nude photographs of themselves in return. He accomplished this by introducing himself to the victims as a young woman, suggesting a meeting with his victim, suggesting to each victim that they "trade pics" before meeting, and then sending the victims nude photographs of a young woman who was purportedly the sender of the AIM messages (DE 109:193-96, 208-09, 225-30, 265, 274-75; GX4, GX4.101-4.114, 4.311, 4.401, 4.402, 4.306-4.310). In return, each of the victims sent nude photographs of himself to Beckett

using AIM or an MSN live feed (DE DE109:194-95; 228-30; 286-87 GX4.101-114; GX4.301-305; GX7.107-7.108).

Det. Paige found the nude images that were sent from Beckett, using the name "Chelsea," as well as the nude images his victims sent in return, all organized on the computer under the user name "Timmy" in subfolders entitled "mikewebcam," "cool1,"and "jordan" (DE108:119-32, 134; GX4.101-4.134). The fact that the pornographic images were organized in subfolders under Beckett's user name "Timmy" in a computer seized from his bedroom establishes that Beckett was aware of their existence and had organized them. The fact that Beckett threatened to broadcast the nude images of his victims to their friends on their respective MySpace pages if the victims did not meet him and permit him to perform oral sex (DE109:198-99, 233-36, 255-58, 287), also shows that he was aware that he was in possession of those images.

Beckett was also well aware of the pornographic nature of those images. When one of the victims threatened to go to the police after Beckett threatened to send nude images of the victim to his friends on MySpace, Beckett suggested that might not be in the victim's best interest, since the victim had sent child pornography to Beckett (DE109:200 "And tell them that you send child pornography? Good idea by the way"). Also, when MG disclosed to Beckett that he had Beckett's IP address and that

one of his mother's friends was an attorney who could use that address as evidence, Beckett immediately attempted to return to MG the nude photos that Beckett had recorded from MG's live feed (DE109:238). Beckett's attempt to rid himself of these images strongly suggests that he was aware of the contraband nature of the images.

Moreover, in his post-arrest statement Beckett admitted that he had downloaded child pornography from the internet (DE108:47). Beckett claimed that he had at least 100 images of child pornography as well as 30 movies depicting child pornography on his computer (DE108:47). All of this evidence amply supports the jury's finding that Beckett was in knowing possession of child pornography.

B. Production of Child Pornography, in violation of 18 U.S.C. § 2251(a) (Counts Two through Fifteen)

Beckett also challenges the sufficiency of the evidence to sustain his convictions of production of child pornography, in violation of 18 U.S.C. § 2251(a), as charged in Counts Two through Fifteen of the superseding indictment (Br. at 22-24). He claims that the government failed to produce any evidence to show that the pornographic images, even if produced, would thereafter be transported or shipped in interstate or foreign commerce (Br. at 24). His claims have no merit.

In order to prove a violation of 18 U.S.C. § 2251(a), the government is required to prove that the defendant used, persuaded, induced, enticed, or coerced a minor to

engage in sexually explicit conduct for the purposes of producing visual depictions of such conduct, knowing that such visual depictions would be transported or shipped in interstate or foreign commerce. *See United States v. Overton*, — F.3d —, 2009 WL 2020527, slip op. at 15 (9th Cir. July 14, 2009); *United States v. Pierson*, 544 F.3d 933, 938 (8th Cir. 2008); Beckett was charged in four counts of production of child pornography on or about July 9, 2007, (Counts Two through Five); four counts of production of child pornography on or about June 2, 2007(Counts Six through Nine); and six counts of production of child pornography on or about June 21, 2007 (Counts Ten through Fifteen). Counts Two through Five relate to the images that JH sent to Beckett; Counts Six through Nine relate to the images that CL sent to Beckett; and Counts Ten through Fifteen relate to the images that CH sent to Beckett.

While these various counts pertain to three separate victims, Beckett employed the same method of operation as to all counts, and the evidence concerning his methods amply supports a finding of guilt on all 14 counts. Beckett persuaded, induced, or enticed minors to engage in sexually explicit conduct for the purposes of producing visual depictions of such conduct. He contacted each of his minor victims on MySpace or AIM and introduced himself as "Chelsea," an attractive 17-year-old girl who was interested in meeting young men. Beckett suggested that "Chelsea" and the victim trade photographs of themselves before meeting in person. Beckett sent

each of his victims nude photographs of a 17-year-old young woman using AIM, and his victims sent him nude photographs of themselves in return.

C. JH (Counts 2, 3, 4, 5)

Beckett communicated with JH on MySpace and AIM (DE109:185-86). When JH expressed some hesitation to meet "Chelsea," Beckett, as Chelsea, suggested that they trade photographs (DE109:193). Beckett stated that there was "only one way to see and that's to trade" (DE 109:193). Beckett proposed that he would send photos to JH and instructed JH "then you send me a couple, OOK. And then maybe some more" (DE109:194). Beckett sent JH photos of a young woman, including some showing the young woman in the nude (DE109:195; GX 4.101-4.114). JH did not have any nude photographs of himself stored on his computer, so he left the AIM chat session long enough to take some photographs (DE109:196). When he was finished, he told Beckett: "Yeah, just took them, sending them to my computer so I can put them up" (DE 109:196). JH sent Beckett four nude photographs of himself (GX4.306-4.310; *see* DE108:130, describing photos as "male exposing genitals"). These photographs were discovered on a computer seized from Beckett's bedroom pursuant to a warrant as well as on JH's computer (DE108:134).

This evidence furnished adequate proof of Beckett's violation of § 2251(a) as to JH. Beckett enticed or induced JH to take nude photographs of himself by

presenting himself as a young woman who was interested in meeting JH, convincing JH that an exchange of photographs would cure any uncertainty JH felt about meeting this young woman, and then transmitting nude photographs of a young woman to JH and requesting that JH send photographs in return. Moreover, the jury reasonably could have concluded from Beckett's instructions to JH about sending photos to Beckett in response to the photos Beckett had sent to JH that Beckett anticipated that JH would use the same electronic means of transmitting the photographs. JH sent the photographs to Beckett using AIM (DE109:194-95). The trial evidence showed that AIM servers are located in Northern Virginia and that all transmissions through AIM are routed though that server (DE108:74). Thus, the evidence also demonstrated Beckett's knowledge that the visual depictions would be transported or shipped in interstate or foreign commerce and they were, in fact, transmitted in interstate commerce.

D. CL (Counts Six - Nine)

Beckett approached CL on MySpace and they continued their correspondence on AIM (DE109:250). Beckett, who initially presented himself as "Chelsea," a 17-year-old girl from the Wellington area of West Palm Beach, sent photographs to CL of a young woman purporting to be Chelsea, including some nude photographs (DE109:265; GX7.102-7.106). CL, thinking he was communicating with a teenage

girl, took nude photographs of himself and sent them to Chelsea over the internet (DE109:270; *see* DE108:130, describing photographs as "male exposing genitals"). These photographs were discovered on CL's computer as well as on the laptop seized from Beckett's bedroom (DE108:132; DE109:155). From the tone and content of Beckett's AIM chat with CL both before and after Beckett revealed that he was a man, not a 17-year-old girl (GX7.1), a reasonable jury could have concluded that Beckett had induced CL to send nude photographs of himself to "Chelsea" if CL wanted to meet "Chelsea." Moreover, the jury could have concluded that Beckett anticipated that the photos would be shipped or transported in interstate commerce. CL and Beckett were communicating on AIM and it was reasonable for the jury to conclude that Beckett expected that CL would transmit the photos through that medium. Since all of AOL's servers are located in Virginia, the images necessarily traveled in interstate commerce.

E. CH (Counts Ten - Fifteen)

Beckett, as "Chelsea," contacted CH on MySpace and they continued their communications on AIM (DE109:274, 295). Beckett appeared interested in meeting CH and inquired, "could u sneak out for like an hour tonight?" (GX4.311). The ensuing conversation established that an exchange of photographs was a prerequisite to CH meeting "Chelsea" (DE109:274; GX4.311). Beckett inquired, "U wanna trade

some pics first?" (GX4.311). When CH replied that he did not have a camera, Beckett suggested, with some urgency, that CH use a camera phone or a web cam:

> yesurifnotcuter: don't u have a camera cell phone?
>
> Kooll1: nope I left it on the roof of my cousins car 2 days ago.
>
> yesurifnotcuter: no webcam nothing =(something !!! lol Come on baby, im horny hehe.
>
> Kooll1: damn
>
> yesurifnotcuter: plzz

(DE109:278-79; GX4.311). Beckett then sent a message that he would send photos to CH, but expected CH to send photos of himself in return "so I can pick u up and have some fun" (GX4.311). Using an old cellular phone, CH took nude photographs of himself and then sent Beckett six nude photographs of himself before Beckett picked him up at his parents' house (DE109:291; GX4.3, 4.301-4.305; *see* DE108:130, describing photos as "male exposing genitals"). These photos were discovered on the laptop seized from Beckett's bedroom (DE108:132).

This evidence adequately proved Beckett's violation of § 2251(a) as to CH. Beckett enticed or induced CH to take nude photographs of himself and transmit them to Beckett by presenting himself as a young woman who wanted CH to "sneak out" for an hour (GX4.311). Beckett made it clear that an exchange of photographs was

a prerequisite to their meeting, however. Beckett instructed CH to send photographs in reply to the photographs that Beckett had sent; Beckett would then pick up CH and they would "have some fun" (GX4.311). A reasonable jury could have concluded that Beckett knew that the images would be transported or shipped in interstate or foreign commerce. The evidence showed that Beckett sent the nude images of the young woman to CH over AIM and instructed CH, "but u can send back" (GX4.311), which established that Beckett intended that the nude photographs be sent to him by the same electronic means he had used to send the photographs to CH. Moreover, when CH initially explained to Beckett that he no longer had a camera, Beckett suggested other electronic means of taking and transmitting the requested photographs (GX4.311: "don't u have a camera call phone?" and "no webcam nothing =(something!!! lol").

While Beckett may not have specifically stated to each of his victims that he expected them to send nude photographs in return, the jury reasonably could have drawn that inference from both the context of the request and the content of the photographs the victims received from Beckett as "Chelsea. " Beckett sent nude photographs of a young woman to each of his victims. The content of Beckett's internet chats with each of his victims was sexual in nature. For example, Beckett asked MG about his genital size and whether or not he liked oral sex before he

suggested that they exchange photographs (DE109:225-26). As one of his victims testified: "It was implied. Especially when they were asking me for head" (DE109:211).

F. Coercing a Minor, in violation of 18 U.S.C. § 2422(b) (Counts Sixteen through Nineteen)

Beckett argues that there was insufficient evidence to support his convictions of coercing a minor, in violation of 18 U.S.C. § 2422(b), as charged in Counts Sixteen through Nineteen (Br. at 23). He argues that "all of the victims were ready, willing, and able, and had in the past, exchanged both photos and sexually explicit chats on-line."[10] There was ample proof to support the charges here.

In order to prove a violation of 18 U.S.C. § 2422(b)[11], the government is required to show: (1) that the defendant knowingly used a facility of interstate

---

[10] The evidence showed that only two of the victims, JH and CL, had previously exchanged nude photos with someone online (DE109:211, 268-70).

[11] 18 U.S.C. § 2422(b) provides, in pertinent part, as follows:

> **(b)** Whoever, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title and imprisoned not less than 10 years or for life.

commerce to attempt to persuade an individual under the age of 18 to engage in sexual activity; (2) that the defendant believed that each of the individuals were less than 18 years old; (3) that if the sexual activity had occurred the defendant could have been charged with a criminal offense under the law of Florida; and (4) that the defendant acted knowingly and willfully. *See United States v. Murrell*, 368 F.3d 1283, 1286 (11th Cir. 2004).

In this case, the government's proof satisfied each of the elements. Beckett used a facility of interstate commerce, AIM (*see* DE108:74). Beckett knew that each of his victims was under the age of 18 because each of them told Beckett his age or the victim's age could be deduced from other information Beckett had seen on the victim's MySpace page (DE109: (JH); GX4.311 (CH); DE109:226 (MG); DE109:245-46 (CL))[12]. And Beckett knowingly attempted to persuade, induce, entice or coerce each of his victims to engage is sexual activity for which any person can be charged with a criminal offense - that is sexual battery under Florida law (*see*

[12] In the transcript of the recorded conversation, CH specifically told Beckett that he was 17 (GX4.311); MG testified that before he sent photos of himself to "Chelsea," he told her that he was 16 (DE109:226, 243); CL testified that he was 16 at the time, and his age was posted on his MySpace page through which Beckett contacted him (DE109:245-46), and during his online chat Beckett asked CL's age and CL replied "16" (GX7.1 "ur age is what again?" "16 "); and the MySpace profile for JH, who was 17 at the time, reported that JH was in high school (DE109:207).

DE108:51; DE198L376-77[13]). As soon as Beckett received the nude photographs from each of his victims, he immediately replied with an e-mail that revealed for the first time that he was a man and threatened to broadcast all of the nude photographs the victim had sent him to the victim's friends on MySpace if the victim did not meet Beckett and permit Beckett to perform oral sex on him.

The victims took Beckett's threats seriously. JH felt "panicked" (DE109:199). He continued his chat for quite some time after Beckett made his demands and even offered to pay Beckett $400 or $500 if Beckett would relent (DE109:202-04, 208). CL was "scared and surprised" (DE109:255). He continued his chat with Beckett for more than half an hour and continually refused to meet Beckett while he attempted to convince Beckett to change his mind about distributing the nude photographs CL had sent to him (GX7.1). Although MG initially thought that Beckett was joking when he revealed to MG that he was a man, not a young woman, MG quickly realized that Beckett was serious (DE109:232-34). MG knew that Beckett had a list of all of MG's friends on his MySpace page, and he saw the tone of Beckett's messages

[13] The court instructed the jury that, as a matter of law, any act by the defendant in which a sexual organ of one of his minor victims would have penetrated or had union with the mouth of the defendant constituted sexual battery of a minor under Florida law.

become increasingly aggressive (DE109:232). CH was "terrified" and did not use the internet for several days thereafter (DE109:287).

From this evidence a reasonable jury could have concluded that Beckett had knowingly and willingly used a facility of interstate commerce to attempt to persuade an individual under the age of 18 to engage in sexual activity that would have been a violation of a Florida criminal statute. The fact that two of Beckett's victims may have previously exchanged nude photographs with young women over the internet on a single occasion (*see* DE109:211, 268-69) is of no moment. At most, that evidence established that the exchange of nude photographs over the internet is not unusual. To the contrary, the frequency with which such activity occurs may have made it easier for Beckett to solicit the photographs that he ultimately used in his attempts to coerce the young men into engaging in illegal sexual acts.

Conclusion

For the foregoing reasons, the district court's decision should be affirmed.

Respectfully submitted,

Jeffrey H. Sloman
Acting United States Attorney

By: _____
Kathleen M. Salyer
Assistant United States Attorney

Anne R. Schultz
Chief, Appellate Division

Lisa Tobin Rubio
Assistant United States Attorney

Of Counsel

Certificate of Compliance

This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 12, 722 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements for Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally-based typeface using Corel Word Perfect 9, 14-point Times New Roman.

Certificate of Service

I hereby certify that an original and 6 copies of the foregoing Brief for the United States were mailed to the Court of Appeals via Federal Express this 21st day of August 2009, and that, on the same day, the foregoing brief was electronically uploaded to the Eleventh Circuit Court of Appeals' Internet web site at www.ca11.uscourts.gov (see attached Brief Upload Result Page), and mailed via United States mail to Jack A. Fleischman, Esq., 2161 Palm Beach Lakes Blvd., Suite 403, West Palm Beach, Florida 33409.

Kathleen M. Salyer
Assistant United States Attorney

ab