UNITED STATES COURT OF APPEALS
ELEVENTH CIRCUIT
CASE NO: 09-10579-BB

****

UNITED STATES OF AMERICA

Plaintiff/Appellee,

vs.

TIMOTHY BECKETT,

Defendant/Appellant.

****

On Appeal from the United States District Court

For the Southern District of Florida

INITIAL BRIEF OF APPELLANT

Fleischman & Fleischman, P.A.
Jack A. Fleischman
2161 Palm Beach Lakes Bd.
Suite 403
West Palm Beach, Florida 33409
561-585-3666 / Fax 561-471-8343
Email: fflaw@yahoo.com
FBN: 0714534
Counsel for Appellant

U.S. COURT OF APPEALS FOR THE ELEVENTH CIRCUIT
CERTIFICATE OF INTERESTED PERSONS
AND CORPORATE DISCLOSURE STATEMENT

United States of America vs. Timothy Beckett, Dkt No. 09-10579-BB

Pursuant to 11th Cir. R. 26.1, the following is an alphabetical list of the trial judge, attorneys, persons, firms, partnerships and corporations that have an interest in the outcome of this particular case and appeal:

1. Timothy Beckett, defendant/appellant.

2. Jack A. Fleischman, counsel for the defendant at trial level, and counsel for the defendant at the trial and appellate level.

3. Honorable Kenneth L. Ryskamp, United States District Court Judge, Southern District of Florida, presiding Judge at trial level.

4. Lothrop Morris, AUSA, counsel for the Government at the trial level.

5. United States Attorney's Office, Criminal Appeals Division, counsel for the appellee at the appellate level.

6. United States of America, Plaintiff/Appellee.

Fleischman & Fleischman, P.A.
2161 Palm Beach Lakes Bd.
Suite 403
West Palm Beach, Florida 33409

_____

Jack A. Fleischman, Esquire
Counsel for Appellant
Florida Bar Number: 0714534

STATEMENT REGARDING ORAL ARGUMENT

The appellant requests that the matter be set for oral argument, as the issues presented in support of appellant's position that his judgment and sentence be reversed can be argued in more depth through argument before the court.

CERTIFICATE OF TYPE AND SIZE

The type and size used in this brief is 14 point Times New Roman.

TABLE OF CONTENTS

TABLE OF CITATIONS

STATEMENT OF JURISDICTION

Federal subject matter jurisdiction exists in this case pursuant to 26 U.S.C. Section 841 (a) (1) and (b) (1) (A) (iii).

Appellate jurisdiction lies pursuant to 18 U.S.C. Section 3742 and 28 U.S.C. 2106, and Title 28 United States Code, Section 1291.

The district court imposed final judgment on February 2, 2009. Appellant filed Notice of Appeal on February 4, 2009. This appeal is timely pursuant to F.R.A.P. 4(b).

STATEMENT OF THE ISSUES

1. Whether the district court erred in denying the appellant's motions to suppress.

2. Whether the district court erred in finding that the evidence was sufficient to convict the appellant for the charges contained in the instant indictment.

STATEMENT OF THE CASE

A. COURSE OF PROCEEDINGS AND DISPOSITION BELOW

The appellant was the subject of a twenty count superseding indictment, alleging multiple counts of production of child pornography, possession of child pornography, and coercion of a minor to engage in unlawful sexual acts. in violation of 18 USC 2251(a), 18 USC 2252A(a)(2)(A), 18 USC 2252A(a)(5)(B), 18 USC 2252A(b)(2), 18 USC 2252A(b)(1), and 18 USC 2422(b). (DE 34)

Pretrial motion to suppress

Pretrial, the defendant filed motions to suppress, attacking the initial collection of information and material collected without subpoena, pursuant to the Electronic Communications Privacy Act, 18 USC 2703, and a motion to suppress evidence outside of the search warrant, which was later issued. The government filed responses to the appellant's motions. (DE 13, 14, 22, 25, 42) All information leading to the appellant and his subsequent arrest came initially from the evidence collected as a result of the information and material collected without subpoena. (DE 31 – pg 50, 64)

At a hearing before the magistrate on the motions, law enforcement testified that they had sought information which led to the development of the appellant as a suspect, from AOL, MySpace, Bellsouth, T-Mobile, AT&T, and Comcast, without a subpoena, either through the use of letters or forms, outlining why emergency and or exigent circumstances existed to proceed without a subpoena, and that a subpoena would follow within five days. An emergency circumstance listed was that the suspect had lengthy and dangerous criminal record, which the detective admitted Beckett did not. On the Comcast application-form, where law enforcement was to describe in detail what the circumstances are which would require the records without subpoena, the detective simply wrote "yes" rather than spelling out the specifics of what the alleged threats were. The detective also represented that subpoenas would be issued within five days, but ended up not having them issued until two and a half weeks later. The detective also felt that the alleged victims had been threatened during the chats, that other unknown victims were possible, and that child pornography had been sent and or received. (DE 31 – pg 45-50, 64-67) Related to the issue of whether some of the evidence collected by law enforcement fell outside the scope of a search warrant later issued, the detective testified that specific language was not

included in the search warrant which stated that law enforcement could actually enter into and access the contents of storage devices sought to be collected in the search warrant, although law enforcement discussed its intention to conduct forensic exams at a later time. (DE 31- pg 52, 67)

Along with arguing that emergency, or dangerous circumstances existed, the government argued that 18 USC 2702 and 2703, did not allow the appellant to seek a suppression remedy, and that the only remedy would be civil remedies, thereby explicitly or implicitly excluding suppression as a remedy. The appellant argued that the fact that Congress included specific language as to when law enforcement could proceed without subpoena, a violation of the procedure would therefore allow for a defendant to seek suppress whether it be termed a fourth amendment violation or relief through U.S. code or statute. (DE 31 – pg 68-76)

On February 19, 2008, the magistrate issued a report and recommendation, denying the appellant's motions to suppress, finding that 2702 and 2703 did not allow for an suppression remedy, and that law enforcement did not exceed the scope of the search warrant by searching the storage devices seized without having obtaining an additional search

warrant to do so. (DE 28) The appellant timely filed objections to the report and recommendation, to which the government responded, the objections of which were overruled by the district court. (DE 30, 32, 33)

The trial

Following jury selection, the parties appeared before the district court for jury trial on November 3, 2008. The government presented four alleged victims, JH, MG, CL, and CH. All told similar stories. While on MySpace, each was approached on line by a 17 year old female, presented to them as "Chelsea", who engaged in conversation, both sexual, and non sexual with them, and exchanged pictures with them, that is the alleged victim would send "Chelsea" a nude or semi nude picture of themselves, and in some cases, "Chelsea" would send the same picture back. At some point in the conversations, "Chelsea" would disclose that she was really a male, and that if the alleged victim did not engage in oral sex with him, he would send the pictures that the alleged victim had sent him, to the alleged victim's other posted friends on MySpace. (DE 109 – pg 187-189, 192-196, 198-199, 218, 227-229, 232-234, 248-249, 255, 274-275, 280, 286)

In addition, CL informed his parents and filed an online complaint. CL also received a phone message on his cell phone voicemail, which was later identified as the appellant. (DE 108 – pg 48; DE 109 – pg 259, 265) CH testified that he had actually met the appellant, believing that he was the brother of "Chelsea" coming to pick him up at his home to meet her. Once in the vehicle, CH testified that he took money from the appellant to remove his shirt and to show him his penis, and that the appellant wanted CH to drink alcohol that he had in the vehicle. While driving, a police officer stopped then, and upon learning that the appellant did not have a valid driver's license, and that CH did, CH was allowed to drive the vehicle, and drove himself home. (DE 109 – pg 282-286)

Law enforcement, as well as a pediatrician/child sex abuse expert, testified that pictures and video found on the appellant's computers were child pornography. Law enforcement also testified that during a post *Miranda* interview, the tape of which was played to the jury, the appellant admitted to having child pornography on his computer, although he did say that the allegations in this case were done as a "joke", and that he never intended to send pictures out as he had threatened to do. (DE 108 – pg 41,

46-47, 50-51, 63-64, 114, 109, 117-118; DE 109 – pg 154-155, 167, 174-175; Govt. Exh. 1)

Following testimony of the government witnesses, the government, and the defense rested. Following argument of counsel, the district court denied rule 29 motions. The government moved to dismiss count 20 of the superseding Indictment, which was granted by the district court. (DE 109 – pg 305-307)

The jury deliberated, and convicted the appellant as charged on count 1 through 19 of the superseding Indictment. The appellant was sentenced to 180 months BOP, followed by lifetime probation. (DE 91) Notice of appeal was timely filed on February 4, 2009. The appellant remains incarcerated. This appeal follows. (DE 92)

SUMMARY OF ARGUMENT

1. The district court erred in denying the defendants' motion to suppress for law enforcement having failed to abide by the requirements of 18 USC 2703. A proper remedy for failing to follow the requirements of this statute is suppression of evidence seized, 18 USC 2702, and 2708 not withstanding.

2. The district court erred in denying the defendant's motion to suppress evidence which were the contents of the appellant's computers and

other storage devices. A second search warrant was required because the first search warrant did not authorize law enforcement to enter into and seize the evidence recovered from these devices.

3. The evidence presented by the government as to all counts was insufficient for conviction. A rational trier of fact could not have found the essential elements of the crimes charged beyond a reasonable doubt.

ARGUMENT

1. The district court erred in denying the defendants' motion to suppress evidence located and seized without a search warrant

Standard of Review

This appellate court reviews a district court's denial of a defendant's motion to suppress under a mixed standard of review, reviewing the district court's findings of fact under the clearly erroneous standard, and the district court's application of the law to those facts de novo. United States v. Gil, 204 F.3d 1347, 1350 (11th Cir.), cert. denied, 531 U.S. 951, 121 S.Ct. 357, 148 L.Ed.2d 287 (2000). The facts must be construed in the light most favorable to the government, because it prevailed in the district court. See, United States v. Santa, 236 F.3d 662, 668 (11th Cir. 2000).

Argument

Pretrial, the defendant filed a motion to suppress, arguing that because law enforcement failed to properly follow the requirements of the Electronic Communications Privacy Act, 18 U.S.C. § 2703, all evidence collected by them without a valid warrant or court order should be suppressed. (DE 13, 43) The pertinent portion of the Act, 2703, states that law enforcement may *not* obtain subscriber information from an Internet service provider without a valid search warrant, court order, or subpoena. It reads that:

§ 2703. Required disclosure of customer communications or records

. . .

> **(c) Records concerning electronic communication service or remote computing services. –** (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 to or customer of such service (not including the contents of communications) 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 (d) 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 of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the –

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(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 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).

The exceptions to § 2703 are found in 18 U.S.C. § 2702, allowing disclosure "if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information." Assuming the information provided by the detective in this case was insufficient to believe that failed to give the service provider sufficient information to have found and or believe *that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information*, as would have been required by § 2702, which is the appellant's position, the key question then becomes does the district court have the authority to require suppression of evidence located and seized, as a remedy for violating the statute. The appellant believes the answer to that question is yes.

The magistrate's recommendation directed to this motion, later adopted by the district court that the motion be denied, was premised upon the argument that because there is no Fourth Amendment protection for subscriber information, the appellant would not be entitled to suppression of evidence as a remedy. See, 18 U.S.C. § 2708

Congress specifically laid out how and when information under the Electronic Communications Privacy Act may be gathered by law

enforcement with, and without a warrant or other court order. Had there been no thought that some protection be afforded the material kept by these service provider companies, such as subscriber information, then there would have be no need for the implementation of § 2703 in the first place. Clearly, the public does not want, and has a constitutional interest in, the government not being granted the ability to go on fishing expeditions for information, which is reflected in the requirements of the statute in requiring a warrant or court order, *unless* the emergency circumstances per § 2702 are present. the Fourth Amendment has been held to limit the scope of investigatory power exercised by federal and state agencies, and to limit the scope of administrative subpoenas. See, See v. City of Seattle, 387 U.S. 541, 544, 87 S.Ct. 1737, 1740, 18 L.Ed.2d 943 (1967); Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 208-11, 66 S.Ct. 494, 505-07, 90 L.Ed. 614 (1946). See, also, FTC v. Am. Tobacco Co., 264 U.S. 298, 306, 44 S.Ct. 336, 337, 68 L.Ed. 696 (1924) ("It is contrary to the first principles of justice to allow a search through all the respondents' records, relevant or irrelevant, in the hope that something will turn up."). In failing to follow the requirements for the collection of evidence pursuant to § 2703, without a warrant or court

order, law enforcement violated the 'unreasonable search' provision for Fourth Amendment exclusionary purposes. The purpose behind the exclusionary rule is not just to bar untrustworthy evidence, ***but to deter police misconduct***. See, e.g., Michigan v. Tucker, 417 U.S. 433, 94 S.Ct. 2357, 41 L.Ed.2d 182 (1974) In the instant case, the detective misrepresented in the requests to the service providers the information which allows each in the first place to provide information with the necessity of obtaining, and being served with a warrant or court order. Additionally, the warrant which the detective stated would be forthcoming in five days, was not issued and delivered until two and a half weeks later. (DE 31 – pg 45-50, 64-67) The gathering of the information from the service providers rising to the level unreasonable search, the district court had available to it the ability to suppress the evidence collected. In applying the law to the facts that exist in the instant case, the district court erred in adopting the report and recommendation of the magistrate to deny the defendants' motion to suppress on this issue.

2. The district court erred in denying the defendants' motion to suppress evidence located and seized from the appellant's computer based upon a search beyond that which was authorized in the search warrant

Standard of Review

This appellate court reviews a district court's denial of a defendant's motion to suppress under a mixed standard of review, reviewing the district court's findings of fact under the clearly erroneous standard, and the district court's application of the law to those facts de novo. United States v. Gil, 204 F.3d 1347, 1350 (11th Cir.), cert. denied, 531 U.S. 951, 121 S.Ct. 357, 148 L.Ed.2d 287 (2000). The facts must be construed in the light most favorable to the government, because it prevailed in the district court. See, United States v. Santa, 236 F.3d 662, 668 (11th Cir. 2000).

Argument

Pretrial, the defendant filed a motion to suppress, arguing that the search warrant obtained a used by law enforcement to collect the appellant's computers and storage devices, did not also authorize the search of the information stored in the computers and other storage devices, and that therefore the evidence collected from the computer and storage devices should be suppressed. (DE 14, 42)

The search warrant did not actually authorize law enforcement to search the contents of the computer or other items, but rather authorized only the

seizure of the computer equipment, hardware, and software. The detective testified during the suppression hearing that *"Q. Is there specific language in the search warrant that says law enforcement can actually enter into and access the contents of those storage devices?* ***A. No.****"*

The appellant respectfully disagrees with the report and recommendation, and the district court's order adopting same, that the motion was properly denied as to this issue because "the search of the computer files was functionally described in the warrant" (DE 28 – pg 11) A review of the search warrant shows that the search warrant did not actually authorize law enforcement to search the contents of the computer or other items, but rather authorized only the seizure of the computer equipment, hardware, and software. This specific language, even if interpreted broadly by the officers executing the warrant, clearly did not entitle the government to undertake a full search and seizure of all the information stored in the computer or related equipment.

Lawful search warrants do not allow for a general exploratory search to be performed with the hope of discovering evidence of a crime. Lawful warrants must be directed towards specific objects in it believed to be instrumentalities by which the crime charged was to have been committed.

See, eg., Gurleski v. U. S., 405 F.2d 253, 258 (5 Cir. 1968). In U.S. v. Mitchell, 565 F.3d 1347 (11th Cir. 2009), the court held that a three week delay in obtaining a search warrant to search the contents of a defendant's computer hard drive, even where the defendant himself gave law enforcement probable cause to initially sieze the computers without a warrant, required suppression. The court noted that "Computers are relied upon heavily for personal and business use. Individuals may store personal letters, e-mails, financial information, passwords, family photos, and countless other items of a personal nature in electronic form on their computer hard drives. Thus, the detention of the hard drive for over three weeks before a warrant was sought constitutes a significant interference with Mitchell's possessory interest. Nor was that interference eliminated by admissions Mitchell made that provided probable cause for the seizure. As the United States magistrate judge observed: "A defendant's possessory interest in his computer is diminished but not altogether eliminated by such an admission for two reasons: (1) a home computer's hard drive is likely to contain other, non-contraband information of exceptional value to its owner, and (2) until an agent examines the hard drive's contents, he cannot be

certain that it actually contains child pornography, for a defendant who admits that his computer contains such images could be lying, factually mistaken, or wrong as a matter of law (by assuming that some image on the computer is unlawful when in fact it is not).” *United States v. Mitchell*, CR407-126, 2007 WL 2915889, at *7 (S.D.Ga.2007).”

Likewise, the material seized was from the appellant’s shared home (DE 31 – pg 45-46), and as such could have contained information that belonged to numerous people, or material that would not be considered contraband. In the instant case, allowing law enforcement to search the hard drive and storage devices of appellant, without the permission to do so being included in the initial search warrant, would amount to allowing the execution of a warrant for a general exploratory search, rather than for what the application for, and warrant allowed, that is the seizure of the computer equipment, hardware, and software. Any further exploration of the storage devices beyond that required an application for, and issuance of, a second search warrant. The district court erred in adopting the report and recommendation of the magistrate to deny the defendants’ motion to suppress on this issue.

3. The evidence presented by the government was insufficient to convict appellant on this Indictment

Standard of Review

Review of sufficiency of the evidence is de novo, drawing all reasonable inferences in the government's favor. United States v. Bowman, 302 F.3d 1228, 1237 (11th Cir. 2002).

Argument

A review of the evidence in the light most favorable to the government would find that any rational trier of fact could not have found the essential elements of the crimes charged beyond a reasonable doubt. Jackson v. Virginia, 443 U.S. 307, 319, 99 S.Ct. 2781, 2789, 61 L.Ed.2d 560 (1979). At the close of all the evidence the appellant moved for JNOV which was denied by the court. The JNOV was again timely raised through his post trial motion. (DE 109 – pg 305-307; DE – 74)

The possession of child pornography

The possession charge required the government to prove that Beckett knowingly possessed or attempted to possess child pornography. While the government did prove that child pornography was found on the appellant's hard drive and other storage devices, the government failed to prove that the

appellant “knowingly” possessed the contraband material. While the government did present testimony that some of the child pornography had been directed to folders that had to be set up by somebody, and would not be named “porn” for example by the computer manufacturer, no witness of the government was able to say that the appellant actually downloaded the child pornography and thereafter stored the material himself (DE 109 – 163-165; 184), nor does Beckett in his statement, in which he does admits to knowing of the photos, admit that the photos and video for which he was later indicted were knowingly downloaded and stored by him. See, eg., United States v. Stulock, 308 F.3d 922, 925 (8th Cir.2002) (“one cannot be guilty of possession for simply having viewed an image on a web site, thereby causing the image to be automatically stored in the browser's cache, without having purposely saved or downloaded the image”)

The production of child pornography and coercion counts

The production charges required the government to prove that the appellant knowingly and intentionally employ, use, persuade, induce, entice, and coerced, the minor alleged victims, to engage in sexually explicit conduct for the purpose of producing visual depictions. The coercion counts required the government to prove that the appellant did knowingly attempt to

coerce, persuade, induce, or entice, the minor to engage in sexual activity. Based upon the totality of what was presented, the government failed to meet its burden as to these counts. The government failed to prove that the appellant enticed any of the alleged victims to create, and thereafter send to him, pornographic pictures. Further, all of the alleged victims were ready, willing, and able, and had in the past, exchanged both photos and sexually explicit chats on-line. For example, while appellant had indicated to JH that he wanted to exchange pictures with him, he had never told JH to send him nude photos or videos. JH had previously exchanged sexually explicit photos and chats, and he was willing to send out photos to "girls". MG misrepresented his age as 18 years old, had sexual statements posted on his MySpace page, and so long as MG was speaking with a female, he was more than willing to send out nude photos of himself. CL had traded sexually explicit photos and chats with others prior to this incident, and had no problem with taking and sending sexually explicit photos so long as it female was on the other side. CH testified that had the appellant been a female, he would have been willing to meet her. (DE 109 – PG 210-212, 240-242, 268-270, 293-294)

Finally, directed to the production counts, there was no evidence submitted by the government that even if produced, Beckett thereafter knew or had reason to know that "such visual depictions would be transported or shipped in interstate or foreign commerce". There was absolutely know evidence that the appellant ever intended to actually "produce" child pornography for the purpose of thereafter shipping the depictions in interstate or foreign commerce. The depictions produced were in some cases the same pictures sent to appellant by the alleged victim, and there is absolutely no evidence that the appellant thereafter sent any of the photos or video out over the internet as he had stated he would in the chat sessions. (DE 109 – pg 195, 210-212, 242, 293)

Viewing all the evidence in the light most favorable to the government, and drawing all reasonable inferences in its favor, a rational trier of fact could not have found the essential elements of the crimes charged beyond a reasonable doubt. Jackson v. Virginia, 443 U.S. 307, 319, 99 S.Ct. 2781, 2789, 61 L.Ed.2d 560 (1979); United States v. Reme, 738 F.2d 1156, 1160 (11th Cir.1984) The district court erred in denying the appellant's motions for judgment of acquittal.

CONCLUSION

The appellant, Timothy Beckett, submits that based upon the above stated argument, the judgment and sentence in the instant case should be reversed.

FLEISCHMAN & FLEISCHMAN, PA..
Jack Fleischman
2161 Palm Beach Lakes Bd., Suite 403
West Palm Beach, Florida 33409
561-585-3666 / Fax 561-471-8343
Email: fflaw@yahoo.com

/s/ Jack A. Fleischman
By: Jack A. Fleischman
Florida Bar Number: 714534

Certificate of Compliance

I hereby certify that there are 4,282 words contained within this brief from the statement of issues through the certificate of service.

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true and correct copy of the foregoing was furnished this 16 day of July, 2009, by U.S. Mail to: United States Attorney's Office, Appellate Division, 99 N.E. 4th Street, Miami, Florida 33132. Counsel also certifies that the Internet upload of this brief was completed on July 16 and 17, 2009.

By /s/ Jack A. Fleischman
Jack A. Fleischman