

UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

UNITED STATES OF AMERICA)	
)	NO. 3:05-CR-00185
v.)	JUDGE TRAUGER
)	
TIMOTHY RYAN RICHARDS)	
a/k/a CASEY MASTERSON)	
a/k/a ALBERT REDMAN)	
a/k/a CASEY LEE)	

RESPONSE TO MOTION TO SUPPRESS FRUITS OF SEIZURES AND SUBSEQUENT
SEARCHES OF COMPUTER SERVERS

The United States of America, by and through S. Carran Daughtrey, Assistant United States Attorney for the Middle District of Tennessee, and Kayla Bakshi, Trial Attorney for the Child Exploitation and Obscenity Section of the Department of Justice, responds to defendant’s Motion to Suppress Fruits of Seizures and Subsequent Searches of Computer Servers and respectfully requests this Court deny the motion.

Factual Background

1. On September 12, 2005, Magistrate Judge Michael F. Urbanski of the United States District Court for the Western District of Virginia reviewed affidavits for the search of material located on services within the state of California. The material on those servers was related to an ongoing investigation in the Western District of Virginia.
2. Based upon his review of the information presented to him, Magistrate Judge Urbanski approved search warrants for two servers: BlackSun, identified by the Internet Protocol Address 66.54.91.171, Server #4, Cabinet #200.03, at the BlackSun company’s facility

located at 1200 West 7th Street, Los Angeles California, and Neova.net, identified by the Internet Protocol Address 64.71.165.114, Customer # CE0470, Cabinet #341, located in the facilities of Hurricane Electric at 760 Mission Court in Fremont, California. Exhibits A & B.

3. The BlackSun server identified by the IP Address 66.54.91.171 was the server that BlackSun furnished to provide dedicated hosting¹ services to the operator of the Justinfriends sites for use with those sites and/or any other material that the operator maintained. As a result, all of the material on that server was accessible without limit to any and all persons who had access to the Justinfriends material.
4. The BlackSun server identified by the IP Address 66.54.91.171 was not accessible to any other customers of the BlackSun company who made use of the BlackSun company's dedicated, virtual, or co-location hosting capabilities.
5. The Neova.net site was hosted on a server uniquely identified as the server with the IP Address 64.71.165.114 within the co-location² facility provided by the Hurricane Electric company. As with dedicated hosting services customers, the Neova.net server could only be accessed by those having administrative rights to the server and not any or all customers of the Hurricane Electric company.

¹*Dedicated hosting* is a term used to describe a situation in which the web hosting company provides all of the equipment and assumes all of the support and maintenance of a website. Exhibit B, p. 9.

²*Co-location* is a term used to describe a situation in which a server is located at a dedicated hosting facility designed with special resources, such as a secure cage, regulated power, a dedicated Internet connection, online security, and online technical support. Co-location facilities offer customers a secure place to physically house their hardware and equipment. Exhibit B, p. 9.

6. The government began investigating the enterprise associated with the distribution of child pornography via the Justinfriends.com and/or Justinfriends.net websites(hereinafter the “Justinfriends sites”) and related illegal activities in July of 2005.
7. Timothy Ryan Richards was initially identified as being involved with the Justinfriends site from an interviews with an adult male identified as CW1. On September 12, 2005 CW1 was arrested and charged with the production, distribution, sale, receipt, and possession of child pornography and has been detained in federal custody.
8. On September 20, 2005, CW1 provided information to FBI Special Agent Monique Winkis regarding the investigation of the justinsfriends website and the involvement of defendant Timothy Ryan Richards in the distribution, sale, receipt, and possession of child pornography through the Internet.
9. The affidavit for the search warrants for the defendant’s residences and vehicles contained abundant evidence that had been gathered independently of the evidence eventually found by searching the servers. See, for example, Exhibit C, p. 11-13.

Argument

A. *Probable Cause*

Defendant contends that the government exceeded the scope of the warrant by searching material beyond the content found within the subfolders labeled justinfriends.com and/or justinfriends.net on the servers. This argument fails on several grounds.

With respect to the scope of the BlackSun search warrant, the scope was clearly articulated in the Attachment B: Items to Be Seized (Exhibit A, Attachment B) to include “[a]ll content of the

justinfriends.com and/or justinfriends.net servers including any computer files that were or may have been used as a means to advertise, transport, distribute or possess child pornography, in violation of 18 U.S.C. §§ 2252, 2252, and 2252A as well as child pornography images.” In this way, the “justinfriends.com and or justinfriends.net” is used as an adjective to identify the servers to be seized. It is equivalent to the phrasing, “all content of the servers that host the justinfriends.com and/or justinfriends.net” materials.

This is not just the most plain reading of the language in the warrant, it is also the reading which is the most logical and appropriate under the circumstances. The affidavit for the BlackSun server contained a detailed account of some of the major investigative findings that furnished probable cause that a commercial venture surrounded the Justinfriends sites. Exhibit A, pp. 12 - 21. Moreover, the affidavit included information from the affiant FBI agent discussing the nature of modern child pornography ventures as including marketing activities and efforts to facilitate mass distribution of materials. Exhibit A, pp. 8 - 10. Taken together, this material provided abundant probable cause that the government would find evidence of criminal acts related to advertising and distribution of child pornography by searching the server that contained the Justinfriends material.

Based upon this probable cause, the government then properly articulated the scope of the search and obtained authorization to search the server for child pornography content as well as evidence related to the business operations associated with the Justinfriends sites including all of the following:

1. All content of the **justinfriends.com** and/or **justinfriends.net** servers at BlackSun that were or may have been used as a means to advertise, transport, distribute, or possess child pornography

2. All business records, in any form, which pertain to the **justinfriends.com** and/or **justinfriends.net** account and its use of IP address 66.54.91.171, to include all email, ICQ communications, log files of any and all activity, or other communications sent by or received by the account holders, directly or indirectly, whether saved or deleted, and any and all credit card numbers or other methods and identifies used to pay for the account including, but not limited to:
 - a.. E-mail and other correspondence between BlackSun and the individual or entity that created and/or controls the websites known as the **justinsfriends.com** and/or **justinfriends.net**;
 - b. any and all transactional records including File Transfer Protocol (FTP) if available, HTTP logs, port 80 logs, and logs including the dates and times the customer uploaded content to the websites known as **justinfriends.com** and/or **justinfriends.net**; and
 - c. any records of customer service complaints made to BlackSun concerning the websites known as **justinfriends.com** and/or **justinfriends.net**
 - d. any records of subscribers to the **justinfriends.com** and/or the **justinfriends.net** website(s).

Exhibit A, Attachment B.

As a result, the appropriate scope of the government's does not end after it checks files name that actually contained "Justinfriends" in the title. Evidence of advertisements from other websites to the Justinfriends websites might be found in any of the other websites housed on the server. Likewise, email correspondence and log records might appear in other directories that would provide

information about the business dealings between defendant and other parties. Moreover, as articulated in the Sixth Circuit case Guest v. Leis, the government can legitimately check to see what the contents of directories contain – irrespective of the labels on the directories; otherwise suspects would be able to shield evidence from a legitimate search simply misfiling it in a folder with a decoy filename. 255 F. 3d 325, 335 (6th Cir. 2001). In sum, the government has authority to search beyond the files with the names “Justinfriends” in the title: (1) in an attempt to uncover Justinfriends material from within mis-labeled files, and (2) to check other parts of the directory to uncover additional evidence associated with the business venture of the Justinfriends websites.

With respect to the Hurricane Electric/Neova.net server, the technical structure was different but the result is the same. The server that housed the Neova.net materials was co-located within the Hurricane Electric Facilities. As explained in the affidavit, “[c]o-location’ means that a server is located at a dedicated hosting facility designed with special resources, such as a secure cage, regulated power, a dedicated Internet connection, online security and online technical support. Co-location facilities offer customers a secure place to physically house their hardware and equipment.” Exhibit B, p. 9. The warrant related to the search of the identified server for material related to the Neova.net website and described the scope of the search to include the following:

1. All content of the **NEOVA.NET** servers at Hurricane Electric, 760 Mission Court, Fremont California, 94539 including computer files that were or may have been used as a means to advertise, transport, distribute, or possess child pornography
2. All business records, in any form, which pertain to the **NEOVA.NET** account and its use of IP address 66.54.91.171, to include all email, ICQ communications, log files of any and all activity, or other communications sent by or received by the

account holders, directly or indirectly, whether saved or deleted, an any and all credit card numbers or other methods and identifies used to pay for the account including, but not limited to:

- a.. e-mail and other correspondence between Hurricane Electric and the individual or entity that created and/or controls the website known as **NEOVA.NET**
 - b. any and all transactional records including File Transfer Protocol (FTP) if available, HTTP logs, port 80 logs, and logs including the dates and times the customer uploaded content to the websites known as **NEOVA.NET**; and
 - c. any records of customer service complaints made to BlackSun concerning the websites known as **NEOVA.NET**
3. Any and all records related **NEOVA.NET**'s interaction and communication with Gregory J. Mitchel and the websites justinfriends.net, justinfriends.com and mexicofriends.com

As with the BlackSun servers, the government demonstrated probable cause and obtained permission to search the contents of the server that housed the Neova.Net site and related records. Nothing in the Defendant's pleadings point to any infirmity in that authority or search.

B. Scope of the Warrants, General Warrants & Overbreadth

Defendant's second argument is quite similar to its first argument in that it amounts to saying that the scope of the search was too broad because the warrants constituted general warrants or -- in the alternative -- that probable cause was insufficient to justify imaging the servers in their

entirety. In its attempt to support this line of argument, the defense relies on an inaccurate analogy to searching an apartment complex. None of defendant's assertions are tenable given the facts and relevant case law.

Warrants in the Instant Case Are Not General Warrants

The server search warrants in this case do not constitute general warrants. The test for whether sufficient particularity has been offered is context-specific. Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001). The Sixth Circuit held that “[a] search warrant must particularly describe the things to be seized, but the description, whose specificity will vary with the circumstances of the case, will be ‘valid if it is as specific as the circumstances and the nature of the activity under investigation permit.’” Id. (citing United States v. Henson, 848 F. 2d. 1374, 1383 (6th Cir. 1988) quoting United States v. Blum, 753 F.2d. 999, 1001 (11th Cir. 1985). In this context, the government offered 28 paragraphs in each of the search warrant affidavits that described the investigation to that point; and each of those paragraphs delineated separate and significant pieces of evidence related to the criminal enterprise involving the Justinfriends websites and/or the Neova.Net site. That litany justified the government's review of the servers for not only images and content in any or all folders bearing the name “justinfriends” and Neova.Net, but also other parts of the server that would contain evidence like email correspondence, advertising materials, customer inquiries, and other such business materials related to the Justinfriends sites and the Neova.Net site.

Ample Probable Cause to Justify the Scope of the Warrants

Defendant's alternative stance is that the warrants were nonetheless too expansive for the probable cause demonstrated to the magistrate, and that argument must also fail. In United States v. Henson, the Sixth Circuit set forth a standard that allows for the likelihood that defendant might

store information in complex directory structures or use misleading folder name, and such tactics should not thwart proper law enforcement inquiry. In Henson, the court upheld a search warrant in a fraud case that did not specifically denote which files were to be seized, because the inspector “could not have known at the time he applied for the warrant what precise records and files would contain information concerning the odometer-tampering scheme.” Henson, 848 F. 2d at 1383. Along similar lines, the Sixth Circuit, in Guest v. Leis, concluded that the mere act of using decoy file names should not thwart law enforcement. In that case, the court held that the government legitimately may have checked to see that the contents of the directories corresponded to the labels placed on the directories. Otherwise, suspects would be able to shield evidence from a search simply by ‘misfiling’ it. 225 F.3d at 335.

In the instant case, the BlackSun Search Warrant affidavit provides ample description of a relatively sophisticated child pornography business operation that encompassed the “Justinfriends” websites. Having pinpointed the single machine that acted as the server for the Justinfriends websites (identified by the Internet Protocol Address 66.54.91.171), the government had every reason to check to see whether material related to Justinfriends - including evidence of advertising, distribution, and the like - appeared anywhere on the server.

Worth noting is that defendant asserts an inapplicable analogy to an apartment complex. It certainly is the case that the company BlackSun operates like an apartment complex in that it leases server space to customers in the same way that a landlord leases apartments to various tenants. However, the server itself - in this case identified as the machine within the BlackSun facility and as having the Internet Protocol Address 66.54.91.171 - is indeed like a single residence. Just as the government could be granted authority to search an entire residence in which a defendant had

unfettered access to hide a murder weapon, the government was eligible for the same authority in this case. It showed probable cause to believe that evidence related to business operations associated with Justinfriends sites would be found on the server, all of which the operator of Justinfriends - ultimately identified as the defendant – had unfettered access.

Likewise, in the context of the Neova.Net servers, the government identified the machine that was the server containing that site as having the IP Address 64.71.165.114 within facility provided by the Hurricane Electric company. The defense mentions that Hurricane Electric hosts websites for at least 32 businesses. D.E. 81: Motion in Support of Motion to Suppress, n. 4. However, the fact that the Neova.Net material was hosted on a server in a co-location facility does not mean that any of those 32 businesses have access to each other's material such that searching the machine associated with the IP address 64.71.165.114 would result in a search of materials of all 32 customer. Indeed that business practice would defy common sense. Instead, the Hurricane Electric company employee who complied with the warrant was able to pin point the exact location and scope of the material associated with the Neova.Net such that the government could seize and search the correct material. For this reason, no infirmity exists with the search of the server associated with the Neova.Net material.

C. Particularity and Search Protocols

Defendant makes the somewhat redundant argument that the government's search was insufficiently particularized and/or did not utilize appropriate protocols for computer evidence. As described above, the List of Items to Be Seized for each of the BlackSun server (Exhibit A, Attachment B) and the Hurricane Electric server quite clearly delineated the nature of material that

should be searched.³ Moreover, defendant seems to be suggesting that the government should have better used technology to parse out what it needed. As explained above, the nature of the search for the Justinfriends and Neova.Net material was such that it might be found anywhere within the each of the two machines identified as pertaining to this case. In United States v. Upham, the First Circuit handled a case similar to the instance case and upheld a warrant authorizing the seizure of “any and all computer software and hardware, . . . computer disks, disk drives . . .” although defendant objected that the warrant was a “general warrant.” 168 F.3d 532, 535 (1st Cir. 1999). The court noted that “the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the images. A sufficient chance of finding some needles in the computer haystack was established by the probable-cause showing in the warrant application; and a search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for a weapon or drugs.” Id.

D. Authority to Issue Search Warrants

Defendant asserts that the search warrants are void for lack of jurisdiction. The warrant was obtained pursuant to the portion of the Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. §§ 2701-2711 relating to “stored wire and electronic communications and transactional records access.” The plain and unambiguous language of the statute makes “jurisdiction over the offense,” and not the location of the digital information, the basis for judicial authority. For the *issuance* of the warrant, the statute incorporates *the procedures* of the federal criminal rules. The

authority to issue the warrant, however, is created and controlled by the statute itself.⁴

The legislative history of the USA Patriot Act is clear. Largely for the reasons set forth above, Congress intended to allow extra-district authority in three circumstances: search warrants in terrorism cases (Fed. R. Crim P. 41(b)(3)); pen register and trap and trace orders (18 U.S.C. §3123(a)); and warrants for voice mail and electronic evidence (18 U.S.C. § 2703). In *all three* circumstances, Congress required only an offense-nexus as the basis for authority.

Rules of Statutory Construction

Statutory interpretation begins with the plain language of the statute. If clear and unambiguous, the plain meaning of the statute will almost always control, though it may yield in that rare circumstance when Congress clearly expresses a contrary intention. Reves v. Ernst & Young, 507 U.S. 170, 177 (1993); United States v. Turkette, 452 U.S. 576, 580 (1981); Glazner v. Glazner, 347 F.3d 1212, 1214 (11th Cir. 2003); United States v. Grigsby, 111 F.3d 806, 816 (11th Cir. 1997); United States v. Kirkland, 12 F.3d 199, 202 (11th Cir. 1994); United States v. Chandler, 996 F.2d 1073, 1084 (11th Cir. 1993).

There are numerous other rules of construction, sometimes applied in opposition to each other. Courts should generally “look to the language and design of the statute as a whole in

⁴This scheme has practical appeal. From a privacy standpoint, the statute gives certain electronic and other information held by third parties the same protection afforded persons in their home - the barrier of a judicial determination of probable cause. From a venue standpoint, however, the statute gives authority to the court in the district where the offense is being investigated and likely prosecuted. It would make little sense to move this decision to the district where the internet service provider happens to locate its computers, which could be literally anywhere. It would be a waste of resources to require judges, prosecutors and agents to get up to speed on facts and circumstances they do not know, did not develop, and will not revisit, merely because a provider with a significant global internet presence has its server farm in a business park in their district.

interpreting the language at issue.” Chandler, 996 F.2d at 1084 (citing McCarthy v. Bronson, 500 U.S. 136, 139 (1991)). A court may disregard even the plain language of a statute if to do otherwise “would lead to a truly absurd result.” Glazner, 347 F.3d. 1212. An interpretation which renders a phrase a nullity is disfavored, as it offends the rule against attributing redundancy to Congress. Kungys v. United States, 485 U.S. 759, 778 (1988). Title and section headings can help clarify ambiguous language, but should not trump the plain language of a statute. Raven v. Oppenheimer & Co., Inc., 74 F.3d 239, 242 (11th Cir. 1996). Finally, a legislature’s inclusion of particular language in one provision and its omission in another is presumptively deliberate, reflecting an intention that the two provisions have different import or meaning. United States v. Steiger, 318 F.3d 1039, 1050-51 (11th Cir. 2003).

The Plain Language of the USA Patriot Act’s Amendment to ECPA Vested Authority to Issue an ECPA Warrant in the District with Jurisdiction over the Offense, Not in the District Where the Digital Evidence Happens to Be Stored.

The USA PATRIOT Act expanded judicial authority to issue extra-district warrants in certain circumstances. First, Rule 41 was modified to create nationwide search warrant authority for evidence of terrorism offenses. USA PATRIOT Act, Section 219 (creating Rule 41(b)(3), Fed R. Crim. P.). Accordingly, if Congress had also wanted to limit extra-district ECPA warrants to terrorism investigations, it would not have been necessary to amend § 2703 at all, since the limitation would have applied through Rule 41. However, § 2703 was changed as well. Congress switched “*under the Federal Rules of Criminal Procedure ...*” to “*using the procedures described in the Federal Rules of Criminal Procedure ...*” USA PATRIOT Act, Section 220 (emphasis added).

Rule 41(b) is entitled, “Authority to Issue a Warrant.” Generally, that subsection does not *describe procedures for the issuance of the warrant*. Rule 41(d) is entitled “Obtaining a Warrant,”

and could fairly be interpreted to *describe procedures for the issuance of the warrant*. Rule 41(e) is entitled “Issuing the Warrant,” and it clearly *describes procedures for the issuance of the warrant*. Even this minor change to § 2703 suggests that the amendment was not intended to incorporate all of Rule 41, but only those procedural provisions regarding the warrant’s issuance. Rule 41(b)(3) would not be such a provision, since it deals with judicial authority and not procedure.

The Act brought a more significant change, however. It added new language to § 2703 which specifically authorized issuance of an ECPA warrant “by a court with jurisdiction over the offense under investigation.” This is the provision which clearly gave the ECPA warrant extra-district reach. Any contrary interpretation would nullify this language altogether. It would mean that Congress included entirely superfluous language, and would offend the presumption against legislative redundancy.

The plain language of § 2703 is thus inescapably unambiguous. Any court with jurisdiction over the offense may issue an ECPA warrant for electronic evidence located anywhere in the country. The fact that Rule 41(b)(3) also authorizes extra-district warrants in terrorism cases does not take away the authority established in § 2703. By its own terms, Rule 41 cannot “modify any statute regulating search and seizure, or the issuance and execution of a search warrant in special circumstances.” Fed. R. Crim. P. 41(a)(1).

F. Timeliness of the Search

Defendant also asserts a general complaint of timeliness about the government’s search computer evidence. Neither Fed.R.Crim.P. 41 nor the Fourth Amendment provides for a specific time limit in which a computer may undergo a government forensic examination after it has been

seized pursuant to a search warrant. Timeliness usually arises in situations where evidence has not yet been seized and preserved, and as a result, the legitimate “staleness” question of whether the probable cause that existed at one point in the past continues to exist at the later date of a proposed search. Even in the instance of evidence that has not yet been seized and preserved, the staleness standard is flexible and dependent upon circumstances. See United States v. Greene, 250 F.3d 471, 480 (6th Cir. 2001). “Rather, a staleness determination should be flexible,” taking into account the character of the crime, criminal, thing to be seized, and place to be searched. Id. Since the evidence in the instant case has been preserved in its original form since the date of seizure in September 2005, there is no question of whether the probable cause that existed then, continues to exist at this time.

Also, as has been articulated in previous pleadings, digital forensic examiners are in short supply within the federal government. Indeed digital searches are different in kind than physical searches, requiring technical expertise and a great deal of time and delays of several months are often unavoidable. See Orin S. Kerr, Search Warrants in an Era of Digital Evidence, 75 Miss. L.J. 85, 95 (2005). Such delays are not a product of lackadaisical effort from the government but rather prioritization based upon urgency with consideration for the schedule trial date. Defendant in this case jointly moved for a continuance to the October 10, 2006, trial date. As a result, he can not now legitimately expect that the government’s trial preparation be halted on timeliness grounds while the defense uses the next several months to continue to prepare for trial.

G. Fruit of the Poisonous Tree Doctrine

The defendant’s assertion that this Court should suppress the fruits of the searches of the servers fails as well. Most importantly, as described above, the government did not violate the

defendant's rights as asserted in his motion to suppress. Moreover, the basis the search warrant for defendant's residences and vehicles resulted from investigative steps independent of searching the servers. Those steps included interviews with cooperating witnesses, and in particular a witnesses identified as CW1 and "Justin" in the search warrants for the defendant's residences and vehicles. Exhibit C, p.11-14. Indeed the servers had not been analyzed at the time that Richards' residences were searched. The search warrant affidavits for Richards' residences and vehicles articulated the following facts - learned from sources other than the servers data – which justified the search of those premises:

On September 12, 2005, CW1 was arrested and charged with the production, distribution, sale, receipt, and possession of child pornography and has been detained in federal custody.

On September 20, 2005, CW1 provided information to Special Agent Winkis regarding the investigation of the justinsfriends website and the involvement of TIMOTHY RICHARDS in the distribution, sale, receipt and possession of child pornography through the Internet.⁵

CW1 stated TIMOTHY RICHARDS goes by the name of "Casey." CW1 stated he has been in communication on and off with RICHARDS since 1996 when CW1 was a member of RICHARDS' original website named caseysapartment.com which contained child pornography. CW1 has had sporadic contact with RICHARDS through online communications since 1996. CW1 reports RICHARDS lives with a minor boy named "Dew" who CW1 believes to be approximately 14 years old. RICHARDS told CW1 he is having sexual relations with "Dew" and has for the past two years. At the time that RICHARDS told CW1 he was having sex with "Dew," RICHARDS was an adult.

"Dew" has been identified and is a 13 year old boy through a "bio" that is posed on a website called myspace.com, which contains his photograph. Additionally, "Dew" told a Tennessee Department of Children's Services employee that he is 13 years old. The Tennessee Department of Children's Services confirmed that "Dew" appears to be a 13 year old child.

CW1 reports "Dew" was first observed by RICHARDS and CW1 in a website called

⁵ On September 12, 2005, CW1 was arrested and charged with the production, distribution, sale, receipt, and possession of child pornography and has been detained in federal custody. CW1 has provided information under a limited grant of use immunity.

“mylivewebcam.com” and recalls RICHARDS expressing when he observed “Dew’s” image online, “hands off, he’s mine.” This occurred about two years ago when “Dew” would have been approximately 12 years of age. CW1 reports RICHARDS and “Dew” currently live together in Nashville, Tennessee.

CW1 states that RICHARDS has operated child pornography websites since 1996 when RICHARDS was living in Maryland. RICHARDS would “stream in” “Justin’s” live shows which featured “Justin” engaging in sexually explicit conduct to his own website(s). The website(s) would advertise them and make them available through caseyandkylescondo.com. “Justin” would receive free streaming and RICHARDS would benefit from increased membership subscriptions because of these live shows.

CW1 reports RICHARDS has always been interested in obtaining the domain names for the justinsfriends websites because of their popularity and money-making potential. CW1 reports that in or around July of 2005, RICHARDS was not only hosting the website but started operating the website and receiving profits from the website’s membership subscriptions. “Justin” confirms that in or around June of 2005, “Justin” was aware that an increased percentage of the proceeds from the justinsfriends website was being provided to RICHARDS by the payment processor WEBCO.net. At this time, CW1 was also receiving compensation from the site. “Justin” states when he became aware of the extent of the profits that were being funneled by UM1’s company, WEBCO to RICHARDS, he communicated directly to RICHARDS via online communications about it and RICHARDS stated “I’m doing the hosting, I’m doing the advertising, I’m doing everything, so I should get a larger percentage.”

CW1 also reports RICHARDS was aware of the content of the justinsfriends website and knew it contained images of minors engaged in sexually explicit conduct including images of “Justin” when he was a minor. CW1 reports his communication with RICHARDS became more frequent in recent years when CW1 became more involved in child pornography websites such as justinsfriends.com. His communication with RICHARDS continued up until September 12, 2005 when he was actively involved in the operation of the justinsfriends website with RICHARDS. CW1 knew that RICHARDS was aware of “Justin’s” age because CW1 had had direct discussions with RICHARDS about “Justin’s” age and the fact that “Justin” was a minor.

CW1 reports RICHARDS and UM1 have been subjects in an investigation in the Boston, Massachusetts area regarding allegations involving child pornography. Lisa Tuddly, an FBI agent, confirmed that in 2000, RICHARDS and UM1 were both subjects of an investigation in the Boston, Massachusetts area for child pornography related offenses. The investigation was conducted by the Massachusetts Attorney General’s office in conjunction with Somerville Police Department. The underlying investigation revealed an Internet service provider and web hosting company owned and operated by RICHARDS and UM1 called Nimenet.com was hosting child pornography websites. No arrests were made.

“Justin” reports that in or around the Spring of 2005, RICHARDS began exclusively hosting

the justinsfriends website. “Justin” switched web hosting providers from UM1’s business WEBCO.net⁶ (retaining WEBCO’s credit card processing services) to RICHARDS’ web hosting service. In exchange for providing “Justin” with web hosting services RICHARDS received 15% of the proceeds from subscription memberships to the justinsfriends website. In addition, “Justin” reports that RICHARDS has advertised the justinsfriends website on his own websites including caseyandkylescondo.com. In addition, RICHARDS placed a banner advertisement in June of 2005 on the justinsfriends website advertising and providing a link to RICHARDS’ website caseyanddewtv.com. “Justin” also states RICHARDS uploaded videos of “Justin” as a minor engaging in sexually explicit conduct to RICHARDS’ own websites. “Justin” reports RICHARDS knew he was a minor in the videos RICHARDS uploaded and advertised. In addition, “Justin” reports RICHARDS knew and has always known the justinsfriends website provided images of minor boys including “Justin” engaging in sexually explicit conduct and would advertise and market the justinsfriends website with this knowledge for financial gain.

“Justin” states that the justinsfriends website was affiliated with Casey’s websites to include caseyandkylescondo.com and caseyscondo.com. When members signed up for any of the websites they would be asked if they also wanted to join the other associated websites. This advertising increased revenue and membership subscriptions for all websites involved.

“Justin” states RICHARDS encouraged “Justin” to stream his live webcam shows directly to RICHARDS’ websites on a regular basis. It is known in the child pornography industry that websites offering live children engaging in sexually explicit conduct generate more subscriptions than static websites without live feed.

During the investigation, and examination of computer record information revealed that the servers that RICHARDS used to provide web hosting services for the justinsfriends, Caseyandkylescondo.com, Caseysapartment.com, Caseyscondo.com caseyanddewtv.com websites as well others were located at the facilities of BlackSun in California.

BlackSun is an electronic communication service provider and has a colocation facility in Los Angeles, California. Information obtained from BlackSun confirms that RICHARDS leases server space from BlackSun. The justinsfriends.net as well as Caseyandkylescondo.com, Caseysapartment.com and Caseyscondo.com all resolve to the same IP address, 66.54.91.171 which was hosted on RICHARDS’ server located at the BlackSun facilities.

On September 12, 2005, a search warrant was executed on the residence of CW1 and on RICHARDS’ server located at BlackSun. These warrants were executed within hours of each

⁶ The defense correctly points out a typographic error in the residence Search Warrant Affidavit whereby the Neova.net server is sometimes referred to as “Webco.” “Webco” is not the name of a separate company but rather the generic term that law enforcement used as a place holder before determining the appropriate company name/website name of Neova.Net.

other. When law enforcement officers entered CW1's residence, he was involved in an online communication with RICHARDS. CW1 reports RICHARDS was informing him that law enforcement had "raided" RICHARDS' server in California. RICHARDS also informed CW1 that the owner of BlackSun, a friend of his, contacted him to alert him to the law enforcement presence.

During the execution of the search warrant on RICHARDS' server on September 12, 2005, service to the websites was interrupted. At that time, RICHARDS contacted a BlackSun representative who referred him to a Los Angeles FBI agent who executed the warrant on RICHARDS' server. RICHARDS questioned the FBI agent about why the server was off-line and when it would be back on-line. Richard informed the FBI agent that "Zack" (last name unknown) leases four servers from BlackSun but that RICHARDS "subleases" one of the servers – the one that was subject to the search warrant. RICHARDS stated he maintains the server and is in contact with the individuals who own the websites that are on the server. RICHARDS also gave the impression he expected the justinsfriends.com website would go back online.

RICHARDS has been independently identified by the FBI as TIMOTHY RYAN RICHARDS through the Florida Department of Motor Vehicles, in which the photograph on the driver's license was compare to the website images of "Casey." RICHARDS' date of birth is May 16, 1981 and his social security number is 218-04-2376. Richard resides at 5203 Raywood Lane in Nashville, Tennessee 37211.

Dunn and Bradstreet reports indicate that UM1 and RICHARDS are business associates, both of whom are listed for the nimenet web hosting service. Investigative interviews with CW1 as well as information obtained during the Massachusetts Attorney General's investigation indicate that the individuals went to high school together in Maryland and attended college together in Massachusetts.

On September 20, 2005, surveillance was conducted on RICHARDS' residence at 5203 Raywood Lane in Nashville, Tennessee and agents observed RICHARDS exit his vehicle and enter the residence. At that time, agents observed RICHARDS with a teenage boy. Agents also observed a vehicle at the residence and described it as a red sports utility vehicle with Florida tag X00TXB. This vehicle was first observed at the residence on September 18, 2005. The vehicle is registered to TIMOTHY RICHARDS listing the address 30841 Midtowne Court, Zephyrhills, Florida 33544.

Exhibit C. In this way, the defendant's identity was obtained independently based upon information provided by CW1 that Timothy Ryan Richards was involved in the distribution, sale, receipt, and possession of child pornography through the Internet in relation to the Justinfriends sites.

Conclusion

For all of the aforementioned reasons, the government respectfully requests that this court deny the defendant's Motion to Suppress Fruits of Seizures and Subsequent Searches of Computer Servers.

Respectfully submitted,
JAMES K. VINES
United States Attorney for the
Middle District of Tennessee

s/ S. Carran Daughtrey
S. Carran Daughtrey
Assistant United States Attorney
110 Ninth Avenue South, Suite A-961
Nashville, Tennessee 37203-3870
Telephone: (615) 736-5151

Kayla Bakshi
Trial Attorney
Child Exploitation and Obscenity Section
United States Department of Justice
1400 New York Avenue, Suite 6000
Washington DC 20530
Telephone: (202) 353-9881

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing has been served electronically
or by mail to the following:

Peter J. Strianse
Tune, Entekin & White
315 Deaderick Street, Suite 1700
Nashville, TN 37238

Kimberly S. Hodde
Hodde & Associates
40 Music Square East
Nashville, TN 37203

on this, the 19th day of June, 2006.

s/ S. Carran Daughtrey _____
S. Carran Daughtrey