

Case No. 2009-H20

IN THE SUPREME COURT OF THE UNITED STATES

---

UNITED STATES OF AMERICA,

*Petitioner,*

v.

STARTESTS, INC. AND THE COLONIAL FOOTBALL LEAGUE,

*Respondent.*

---

On Appeal from the U.S. Circuit Court of Appeals for the Fourteenth Circuit

---

BRIEF OF PETITIONER

---

Team #7

## **QUESTIONS PRESENTED**

- I. Under Fed. R. Crim P. 41(g) and the Fourth Amendment, does a party constitute a “victim” of a government search for purposes of standing when that search is directed against five specific players that are affiliated with the party by league?
  
- II. Under the plain view exception to the Fourth Amendment warrant requirement, may the government retain evidence discovered during the course of a warranted search and seizure, when that evidence is digital and the government did not commence an unauthorized search?
  
- III. Under the Fourth Amendment, may a warrant authorize the search and seizure of digital evidence when that warrant provides officers with sufficient guidance to conduct a search as well as the latitude to remove electronic materials from the search site when determined necessary by a trained personnel based on inability to retrieve the materials without prolonged stay on the premises?

**TABLE OF CONTENTS**

**QUESTIONS PRESENTED** ..... 1

**TABLE OF CONTENTS** ..... 2

**TABLE OF AUTHORITIES** ..... 3-4

**OPINIONS BELOW** ..... 5

**STATEMENT OF THE CASE** ..... 5-7

**SUMMARY OF THE ARGUMENT** ..... 7-9

**ARGUMENT** ..... 10-30

I. THIS COURT SHOULD REVERSE THE APPELLATE COURT’S  
DECISION TO ALLOW THE 41(g) MOTION BECAUSE CFL IS NOT A  
VICTIM OF AN UNLAWFUL SEARCH AND SEIZURE AND THEREFORE  
LACKS STANDING TO BRING SUCH A MOTION ..... 10

II. THIS COURT SHOULD REVERSE THE FOURTEENTH CIRCUIT’S  
FINDING THAT THE GOVERNMENT CONDUCTED AN ILLEGAL  
SEARCH AND SEIZURE BECAUSE THE FOURTEENTH CIRCUIT  
FAILED TO APPROPRIATELY APPLY THE PLAIN VIEW EXCEPTION  
TO THE GOVERNMENT’S SEIZURE OF DIGITAL EVIDENCE ..... 11

III. BECAUSE THE WARRANT IN QUESTION WAS MADE TO GUIDE THE  
SEARCH OF THOUSANDS OF COMPUTER DOCUMENTS THAT WERE  
HIDDEN, ENCRYPTED, AND DISTRIBUTED OVER SEVERAL  
COMPUTER SYSTEMS, AND BECAUSE THE SAME WARRANT  
PROVIDED ENOUGH INFORMATION TO GUIDE OFFICERS IN THEIR  
SEARCH, THE WARRANT’S AUTHORIZATION ALLOWING OFFICERS  
TO SEIZE MATERIALS FOR LATER SEARCH WITH BETTER  
TECHNOLOGY CAPABLE OF ASCERTAINING THE NECESSARY  
INFORMATION DID NOT VIOLATE THE TENETS OF THE FOURTH  
AMENDMENT’S REQUIREMENT OF PARTICULARITY ..... 22

**CONCLUSION** ..... 31

**CERTIFICATE OF SERVICE** ..... 31

**TABLE OF AUTHORITIES**

CONSTITUTIONAL AMENDMENTS:

U.S. CONST. amend. IV .....22

UNITED STATES SUPREME COURT CASES:

*Alderman v. United States*, 394 U.S. 165 (U.S. 1969).....10

*Arizona v. Hicks*, 480 U.S. 321 (U.S. 1987).....12-13, 19

*Coolidge v. N.H.*, 403 U.S. 443 (U.S. 1971).....12

*Horton v. California*, 496 U.S. 128 (U.S. 1990).....11-12

*Johnson v. United States*, 333 U.S. 10 (U.S. 1948).....11-12

*Jones v. United States*, 362 U.S. 257 (U.S. 1960) .....10

*Rakas v. Illinois*, 439 U.S. 128 (U.S. 1978).....10-11

UNITED STATES COURT OF APPEALS CASES:

*United States v. Adjani*, 452 F.3d 1140 (9th Cir. Cal. 2006) .....15-18

*United States v. Alexander*, 574 F.3d 484 (8th Cir. Mo. 2009).....14

*United States v. Beusch*, 596 F.2d 871 (9th Cir. Cal. 1979).....19

*United States v. Carey*, 172 F.3d 1268 (10th Cir. Kan. 1999).....14, 19

*United States v. Comprehensive Drug Testing, Inc.*,  
579 F.3d 989 (9th Cir. Cal. 2009).....19-21, 26-28, 30

*United States v. Dichiarinte*, 445 F.2d 126 (7<sup>th</sup> Cir. Ill. 1971) .....13

*United States v. Giberson*, 527 F.3d 882 (9th Cir. Nev. 2008).....16-19

*United States v. Hargus*, 128 F.3d 1358 (10th Cir. Okla. 1997) .....23-24

*United States v. Johnson*, 709 F.2d 515 (8th Cir. Minn. 1983) .....23

*United States v. Miranda*, 325 Fed. Appx. 858 (11th Cir. Fla. 2009) .....13-14, 19

*United States v. Schandl*, 947 F.2d 462 (11th Cir. Fla. 1991) .....23-24, 28

*United States v. Shilling*, 826 F.2d 1365 (4th Cir. Va. 1987) .....23-24

*United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. Cal. 1982) .....26, 28

*United States v. Upham*, 168 F.3d 532 (1st Cir. Me. 1999).....22-23, 28-29

*United States v. Wong*, 334 F.3d 831 (9th Cir. Cal. 2003) .....15

UNITED STATES DISTRICT COURTS:

*United States v. Farlow*, 2009 U.S. Dist. LEXIS 112623 (D. Me. 2009).....24-25, 29-30

*United States v. Gleich*, 2003 U.S. Dist. LEXIS 21834 (D.N.D. 2003) .....24

COLORADO STATE CASES:

*People v. Gutierrez*, 2009 Colo. LEXIS 1160 (Colo. 2009).....22, 25-26

## **OPINIONS BELOW**

The opinion of The United States District Court for the District of Wythe (Case No. 2010-W20) is reported at <http://www.wmmootcourt.com/new/wp-content/uploads/2009/04/2010-Spong-Invitational-Problem.pdf>, pages 1-6. The opinion of the U.S. Circuit Court of Appeals for the Fourteenth Circuit (Case No. 2010-W23) is reported at <http://www.wmmootcourt.com/new/wp-content/uploads/2009/04/2010-Spong-Invitational-Problem.pdf>, pages 7-19.

## **STATEMENT OF THE CASE**

Petitioner, United States Government, asks the Supreme Court to reverse the Fourteenth Circuit's decision finding that Respondent, Colonial Football League, had standing to bring a Rule 41(g) claim on behalf of its players for the return of property seized by the government. Further, Petitioner asks the Supreme Court to find that Petitioner lawfully obtained the digital evidence in question under the plain view exception to the Fourth Amendment and to reverse the Fourteenth Circuit's exclusion of the plain view rule. Finally, Petitioner asks the Supreme Court to determine that the federal magistrate properly issued warrants authorizing the Petitioner to seize Respondent StarTests' computer equipment and files for later sorting. Therefore, the Fourteenth Circuit's decision to grant the 41(g) motion in favor of Respondents should be reversed.

In July of 2008, the Federal Bureau of Investigation initiated an investigation into five football players of the Colonial Football League for illegal drug use, namely John (Barry) Reynolds, John Reeves, Danny Rodriguez, Michael Fleming, and Ace Hall. (R. at 7) After discovering a significant amount of evidence of illegal steroid traffic within the professional football league and specifically involving the five named professional football players of the

Wythe City Lightning and Marshal Phoenixes, the FBI learned that the Colonial Football League commenced League-wide drug testing of its players in 2005. (R. at 8) From its collection of eyewitness reports, taped conversations, and other transactional evidence implicating the five star players in steroid trafficking the FBI assembled its demonstration of probable cause of drug use by these players, and applied to District of Wythe magistrate judge for a search warrant to the computer records, files, and equipment related to the Colonial Football League's mandated drug tests. (R. at 8) The drug tests required by the Colonial Football League were administered and stored by the independent business StarTests, Inc. (R. at 1) The Colonial Football League did not otherwise participate in the administration, collection, or storage of the drug testing. (R. at 1) In fact, the Colonial Football League did not even retain access to the results of the drug tests, beyond the report of overall percentage of use within the League. (R. at 1)

The FBI submitted to the magistrate judge of the District of Wythe its affidavit supporting the terms of its warrant application by citing the need to seize and review the computer equipment files based on three assertions. (R. at 2) First the affidavit stated that "the data to be retrieved was massive in quantity, and time would not permit an on-site search." (R. at 2) Second, the file names may be "misabeled or deceptively labeled for confidentiality purposes." (R. at 2) Finally, the affidavit stated that "de-encryption may require software not available on StarTests' computers." (R. at 2)

Magistrate Judge Leon issued the FBI a warrant to search StarTests' facility for computer equipment and storage devices reasonably related to the investigation of the fived specified football players' illegal steroid use. (R. at 8) Additionally, the warrant authorized seizure of the computer equipment or copies of the digital data where on-site search was "impractical." (R. at 2) Magistrate Judge Leon's warrant limited seizures to only that equipment that had been

necessary by “law enforcement personnel trained in searching and seizing computer data” and required “appropriately trained personnel” to review the data. (R. at 2)

Upon search of StarTests’ facility in execution of the warrant, the FBI discovered that StarTests had been conducting drug tests of Colonial Football League players for four years, and the test results were segregated (name from result) and spread across databases on three different computers. (R. at 2) Additionally, Many of the files were indeed encrypted, “while others were hidden in various H- or S- drives.” (R. at 2)

As specified by warrant, the FBI’s head agent determined that search of the digital evidence could take multiple days, and ordered the equipment seized. (R. at 2) Trained computer personnel then searched the three databases to match the test results with the five implicated CFL players. (R. at 2) During this process, the agents also discovered positive test results of other players and decided to copy and retain these positive test results and then returned StarTests’ equipment. (R. at 2)

Respondents Colonial Football League and StarTests filed a Rule 41(g) motion for the return of the copied and retained digital evidence. (R. at 3) Although the District Court for the District of Wythe rejected the motion, the Fourteenth Circuit reversed, granting motion for respondents. (R. at 17) Petitioner has appealed this decision and now asks the Supreme Court to reverse the Fourteenth Circuit’s holding.

### **SUMMARY OF THE ARGUMENT**

This Court should reverse the Fourteenth Circuit’s decision and affirm the District Court of Wythe’s denial of Respondents’ motion under Fed. R. Crim. P. 41(g). Such denial was proper for three reasons. First, Respondent Colonial Football League lacked standing to bring a 41(g) claim against the government. Second, Petitioner United States properly conducted a lawful

search and seizure of property from StarTests' facility, and the digital evidence in question was discovered under the plain view doctrine. Finally, federal magistrates do not offend the mandates of particularity in the Fourth Amendment by granting investigating officers the authority to seize and remove electronic materials for later investigation.

The Colonial Football League's 41(g) motion should have been dismissed because the CFL was not a victim of the search, and because the lower courts relied upon misinterpreted law. Instead of demonstrating how the CFL was an actual victim of the FBI's search, the lower courts appeared to have relied on the "target theory" of standing, which has been explicitly rejected by the Supreme Court. The "target theory" takes the a Supreme Court phrase ("one against whom the search was directed") and gives it a life of its own, when the Supreme Court emphatically states that the phrase is merely a parenthetical equivalent of "victim." However, transforming the phrase into a broader, "target theory" of standing for 41(g), the CFL and lower courts improperly granted standing to the CFL.

Yet beyond the issue of improper standing, the 41(g) motion should have been denied because the digital evidence retained by Petitioner was collected through a lawful search and seizure, and the evidence in question fell under the purview of the plain view doctrine. Because such evidence was discovered during the a single, continuous search in compliance with the warrant, and because CFL and StarTests cannot demonstrate any deviation by the government that could be deemed the commencement of a new, unauthorized search, the District Court of Wythe properly denied the 41(g) motion, and the Fourteenth Circuit's decision should be reversed.

Furthermore, the Fourteenth Circuit improperly barred the application of the plain view doctrine to digital evidence, based on a single untested case of the Ninth District, in the face of

overwhelming precedent to the contrary. Citing some of the very same concerns already dealt with by such contrary precedent, the Fourteenth opted to completely abandon the rule in digital cases instead of dealing with the general difficulties that frequently arise when courts must apply a rule to a specific set of facts. Additionally, the Fourteenth Circuit failed to consider or address the practical costs of complying with the new rule, or how such costs could be dealt with.

Thus, the Fourteenth Circuit improperly administered a bright-line rule, where caution and precedent call for careful application or incremental adjustment. Because the Fourteenth Circuit improperly barred the plain view doctrine from digital cases, this Court should reverse its decision, and deny the Respondents' 41(g) motion.

Additionally, without offending the Fourth Amendment's mandate of particularity, a federal magistrate may issue a warrant that grants investigating officers latitude while conducting a search. Such latitude includes the right to seize computer equipment for later search and sorting when the information contained therein cannot possibly or practicably be obtained during an onsite investigation. Such warrants, however, while offering some latitude to officers, must contain enough information to guide the officers' search. The information contained need not specifically describe every item sought but must contain enough information to ensure that officers are not given authority to rummage through a person's effects looking for unrelated crimes. A warrant that provides general authority to search and seize computers and related equipment but specifies that those materials seized must bear relation to the person or crimes in question is sufficient to meet the requirements imposed by the Fourth Amendment.

## ARGUMENT

### **I. THIS COURT SHOULD REVERSE THE APPELLATE COURT’S DECISION TO ALLOW THE 41(g) MOTION BECAUSE CFL IS NOT A VICTIM OF AN UNLAWFUL SEARCH AND SEIZURE AND THEREFORE LACKS STANDING TO BRING SUCH A MOTION.**

Both the District of Wythe and the Fourteenth Circuit appear to rely on what is known as the “target theory” in finding that the CFL had standing to bring its 41(g) motion. Rather than explaining how the CFL is a “victim” of a search, the District and the Fourteenth repeat the phrase “one against whom the search was directed.” This phrase comes from *Jones v. United States*: “In order to qualify as a person aggrieved by an unlawful search and seizure one must have been a victim of a search or seizure, one against whom the search was directed...” *Jones v. United States*, 362 U.S. 257, 261 (U.S. 1960). However, the Supreme Court in *Rakas v. Illinois*, explains that this quote does not expand the standard to a “target theory” of standing. *Rakas v. Illinois*, 439 U.S. 128, 134-136 (U.S. 1978). Rather, the phrase “one against whom the search was directed” was intended to be a “parenthetical equivalent of the previous phrase ‘a victim of a search or seizure.’” *Id.* The *Rakas* court explicitly rejected any broadened view of “one against whom the search was directed” based on its analysis of *Alderman v. United States*. *Id.* In *Alderman*, the court found no standing to bring a Fourth Amendment claim where persons “who were not parties to the unlawfully overheard conversations or who did not own the premises on which such conversations took place” bring such claims. *Id.* at 136. The court stated its conclusion held firm “regardless of whether or not [such parties] were the ‘targets’ of the surveillance.” *Id.* Therefore, under *Rakas*, a party has no standing to sue unless it can demonstrate it was an actual victim of a search or seizure. *Id.* Furthermore, *Rakas* states that Fourth Amendment rights are personal rights which may not be vicariously asserted. *Id.* at 133-134. Finally, *Rakas* states that a person who is aggrieved by an illegal search and seizure “only

through the introduction of damaging evidence secured by a third person's premises or property has not had any of his Fourth Amendment rights infringed." *Id.*

Because the Supreme Court has explicitly rejected vicarious standing for Fourth Amendment claims, and because CFL is not a victim of a search or seizure, CFL lacks standing to bring its 41(g) motion. Rather CFL's claim amounts to a vicarious assertion of Fourth Amendment rights of others. Just as the defendant's in *Rakas* lacked standing because they did not possess ownership of the car or weapons found in that car when the police searched their vehicle, CFL does not possess ownership of the test results, specimens, or the equipment holding those test results. At most, CFL is a party aggrieved by the search and seizure of evidence secured by a third party's premises or property, and thus, CFL's Fourth Amendment rights were not infringed. Having rejected the expanded rule of standing, the Supreme Court should dismiss the CFL's claim, since the CFL has not demonstrated how the government's warrant, which sought evidence against only five specific players, victimizes the CFL.

**II. THIS COURT SHOULD REVERSE THE FOURTEENTH CIRCUIT'S FINDING THAT THE GOVERNMENT CONDUCTED AN ILLEGAL SEARCH AND SEIZURE BECAUSE THE FOURTEENTH CIRCUIT FAILED TO APPROPRIATELY APPLY THE PLAIN VIEW EXCEPTION TO THE GOVERNMENT'S SEIZURE OF DIGITAL EVIDENCE.**

The Fourteenth Circuit's decision should be reversed because the government properly conducted a lawful search and seizure of players' test results and because the Fourteenth Circuit improperly barred the plain view exception to the digital evidence retained by the government.

The Fourth Amendment affords protections of privacy and security to citizens from unreasonable searches and seizures. *Horton v. California*, 496 U.S. 128, 133 (U.S. 1990). However, the application of the amendment must be viewed in light of the opposing interests it seeks to balance. *Johnson v. United States*, 333 U.S. 10, 13-14 (U.S. 1948). We value both

protections from government intrusion as well as protections from other individuals. *Id.* To this end, the Fourth Amendment must balance our desire for privacy from government with our pursuit of justice and criminal prosecution. *Id.* The plain view exception to the general rule against unwarranted searches and seizures is a tool that helps us maintain an appropriate balance. *Coolidge v. N.H.*, 403 U.S. 443, 467-468 (U.S. 1971).

The plain view exception determines that “under certain circumstances the police may seize evidence in plain view without a warrant.” *Id.* at 465. Of course, the conditions of these seizures are paramount. *Id.* To lawfully conduct a search or seizure under the plain view exception, three conditions must be met. *Horton*, 496 U.S. 128, 136-137. First, the officer conducting the search or seizure must be “lawfully located in a place from which the object can plainly be seen.” *Id.* Second, the officer must have a “lawful right of access to the object itself.” *Id.* Finally, the incriminating character of the item in plain view must be “immediately apparent.” *Id.* These restrictions help ensure that the plain view exception is not used to authorize general exploratory searches that could be used to bypass the Fourth Amendment. *Coolidge*, 403 U.S. 443, 466-467.

A common element of many cases cited by the district court and the Fourteenth Circuit is the commencement of a new, unauthorized search. Where this happens, the search expands beyond the bounds of the plain view exception and enters the realm of illegal/unreasonable search and seizure. *Arizona v. Hicks*, 480 U.S. 321, 323 (U.S. 1987). Thus, conducting a plain view analysis depends largely on a determination of whether and when an officer commenced a separate and distinguishable search from that which was authorized. *Id.* The Supreme Court illustrates this analysis in *Arizona v. Hicks*, where police officers entered defendant’s apartment in response to a gunshot that sent a bullet through the apartment below. *Id.* Police entered the

apartment to look for the shooter, other victims, or weapons, and lawfully seized three weapons and a stocking-cap mask. *Id.* However, during the search of the apartment, one of the officers noticed expensive stereo equipment that did not match the “squalor” of the apartment. *Id.* The officer moved the stereo to read and record serial numbers from the stereo, and then seized the stereo after determining that it was stolen. *Id.* The Supreme Court affirmed the defendant’s motion to suppress the evidence because it concluded that in moving the stereo to read the serial numbers, the officer had commenced a new search, “*separate and apart* from the search for the shooter, victim, or weapons.” *Id.* at 325. By taking “action unrelated to the objectives of the authorized intrusion, which exposed to view concealed portions of the apartment or its contents,” the officer produced a “new invasion of respondent’s privacy [which was] unjustified by the exigent circumstances that validated entry.” *Id.*

Similarly, the Seventh Circuit aptly demonstrates the separate-search distinction in *United States v. Dichiarinte*. *United States v. Dichiarinte*, 445 F.2d 126 (7<sup>th</sup> Cir. Ill. 1971). In that case, the court found the plain view exception inapplicable to the seizure of documents implicating tax fraud because reading these documents was not reasonably necessary to determining the presence of narcotics. *Id.* at 130. Reading the documents constituted the commencement of a separate, general exploratory search, which existed beyond the bounds of the plain view exception. *Id.* at 129.

The new-search distinction is evident even in cases considering digital evidence. In *United States v. Miranda*, the Eleventh Circuit both validated and excluded digital evidence on the basis of whether it was found as part of the authorized search or whether it was discovered after the commencement of a separate search. *United States v. Miranda*, 325 Fed. Appx. 858, 860 (11<sup>th</sup> Cir. Fla. 2009). In that case, an officer obtained a warrant to search an individual’s

laptop for evidence of counterfeiting. *Id.* Files containing child pornography were intermingled with the counterfeiting files, so the officer seized those files. *Id.* The officer then began to search a desktop computer for similar pornographic files, and subsequently seized such files discovered on that computer. *Id.* The court, determining the search of the desktop computer to be a new search not related to discovery of counterfeiting evidence, found the seizure of the tower files to be unlawful, but maintained that those files discovered on the laptop (intermingled with the counterfeiting files) fell squarely within the plain view exception. *Id.*

Likewise, the Eighth Circuit in *US v. Alexander* found seizure of certain digital files lawful under the plain view exception. *United States v. Alexander*, 574 F.3d 484, 490-491 (8th Cir. Mo. 2009). In *Alexander*, the court found that officers had not expanded their search beyond warrant authorization, and although the digital evidence of child pornography was not the evidence sought by the warrant, it was discovered under the plain view exception. *Id.*

Even *US v. Carey*, cited by the Fourteenth Circuit, demonstrates precedent for applying the plain view exception to digital cases. In *US v. Carey*, the Tenth Circuit rejected the application of the plain view where an officer searching a computer for evidence of drug transactions accidentally opened a document containing child pornography. *United States v. Carey*, 172 F.3d 1268, 1271 (10th Cir. Kan. 1999). The officer then began to search the computer for further evidence of child pornography, and the resulting discoveries were suppressed because this search was not part of an authorized search, but rather constituted a new search as well as a temporary abandonment of the original authorized search. *Id.* at 1273. Thus, although the court found the digital files in question were not lawfully seized, they did so by applying the limitations of the plain view exception to those digital files. *Id.* Such application

demonstrates the Tenth Circuit's willingness to adhere to the plain view doctrine even for digital evidence.

The Ninth Circuit (which the Fourteenth purports to follow in *StarTests v. US*) has also traditionally recognized the applicability of the plain view exception to digital evidence. In 2003, *US v. Wong* legitimized the seizure of child pornography under the plain view exception. *United States v. Wong*, 334 F.3d 831, 838 (9th Cir. Cal. 2003). Authorized to search the Wong's apartment for evidence relating to his involvement in murdering his girlfriend, the officers in *Wong* discovered images of child pornography on Wong's computer. *Id.* at 835. The court found the officers were authorized to search Wong's computer for evidence relating to the murder, and determined that the digital evidence of obscenity was lawfully seized pursuant to the plain view exception. *Id.* at 838. Specifically, the files were discovered while the officers were lawfully present, had right of access to the computer files, and could immediately perceive the incriminating nature of the files. *Id.* In reaching this conclusion, the Ninth Circuit attached no cautionary significance to the fact that the incriminating evidence was digital. *Id.*

In 2006, *US v. Adjani* delved into this issue, though it did not explicitly attribute its decision to the plain view exception. In *Adjani*, police officers were authorized by warrant to search the residence of Defendant Adjani for evidence of extortion. *United States v. Adjani*, 452 F.3d 1140, 1142 (9th Cir. Cal. 2006). After seizing Adjani's computer, officers searched and seized the computer of Adjani's co-resident Reinhold where they found digital evidence implicating Reinhold as a co-conspirator in the extortion scheme. *Id.* The Ninth Circuit rejected Reinhold's motion to suppress such evidence, finding that the officer's search of her computer was authorized, since the warrant covered any accessible computers Adjani could have used in committing extortion. *Id.* at 1144. Citing *US v. Beusch*, the Ninth Circuit reiterated that just

because an item seized “happens to contain other incriminating information not covered by the terms of the warrant does not compel its suppression.” *Id.* at 1146. “That the evidence could now support a new charge against a new (but already identified) person does not compel its suppression.” *Id.* at 1151. As in *US v. Wong*, the Ninth Circuit expressed no hesitation to hold the seizure lawful even though the evidence in issue was digital (though it did mention that the new evidence was related to the crime listed by warrant: extortion). *Id.* at 1151. In fact, the Court in *Adjani* stated the fact that digital files could be so easily hidden, mislabeled, or encrypted demonstrated the need for broad search powers regarding such evidence. *Id.* at 1150.

As recently as 2008, in *US v. Giberson*, the Ninth Circuit upheld the seizure of digital evidence where that evidence was not related to the crime covered by the search warrant. In *Giberson*, officers suspected the defendant of producing fake I.D.’s after a traffic stop. *United States v. Giberson*, 527 F.3d 882, 884 (9th Cir. Nev. 2008). The officers obtained a warrant to search Giberson’s home for evidence of fake identification and discovered fake I.D.’s and a personal computer. *Id.* at 885. The officers obtained a warrant to search a mirror copy of the computer’s hard drive for evidence of “records relating to I.D. cards or the creation of I.D. cards.” *Id.* As the officers searched the hard drive, they discovered child pornography. *Id.* As instructed by superiors, the officers continued to search the hard drive for evidence of I.D. cards, and printed out any other files they encountered containing child pornography. *Id.* The court found that the officers did not specifically search for child pornography on the hard drive, and the motion to suppress the evidence of child pornography was properly rejected by the lower court. *Id.* at 889. Discarding Giberson’s argument that computers should be treated differently under the Fourth Amendment because of their capacity to store vast amounts of information, the Ninth Circuit stated “neither the quantity of information, nor the form in which it is stored, is

legally relevant in the Fourth Amendment context.” *Id.* at 888. “While it is true that computers can store a large amount of material, there is no reason why officers should be permitted to search a room full of filing cabinets or even a person's library for documents listed in a warrant but should not be able to search a computer.” *Id.* Finally, the *Giberson* court noted that any attempt to limit Fourth Amendment searches based on the format of stored information would be arbitrary, and that the *Adjani* court had already declared that the intermingling of relevant and irrelevant evidence did not affect the analysis. *Id.*

In the case at hand, the US District Court of Wythe correctly found that the government lawfully seized the digital evidence of players’ test results under the plain view exception. After correctly identifying the need to grant deference to Judge Leon’s decision to issue the warrant, the District Court found the government agents were lawfully present and had lawful access to the seized material. In fact, the District Court relies on *Adjani* to determine that the breadth of the warrant was appropriate in light of StarTests’ complex equipment, databases, and file encryption. As noted above, *Adjani* warned of the dangers of improperly limiting the plain view exception where files could be easily hidden, mislabeled, or encrypted. Such dangers are directly at issue in the case at hand, as the record indicates that many of StarTests’ files were encrypted or hidden in various H- or S- drives.

Given the validity of the warrant, it is clear the digital evidence retained by the government falls within the ambit of the plain view exception. The government was lawfully present and had lawful access to the StarTests’ database results. Furthermore, the nature of the digital data clearly indicates immediately apparent incriminating character, because the tests openly concluded whether players’ tested positive for illegal drug use. Because StarTests and the CFL cannot demonstrate that the government commenced a new, unauthorized search for

evidence of other players' drug use, the evidence retained by the government clearly falls within the plain view exception. The government clearly commenced no such unauthorized search. Indeed, the government's search is hardly distinguishable from that conducted in *Adjani*. Just as the *Adjani* officers' digital search for evidence of extortion produced evidence implicating another person in extortion, here the government's search for digital evidence of five specific players' drug use produced evidence of other players' drug use. There is no reason to distinguish between searching through a hard drive for evidence of extortion (and finding evidence implicating others of the same crime) and searching through a database for evidence of drug use and finding evidence implicating others of the same crime. Since StarTests and CFL cannot define any point where the government commenced a new unauthorized search, the District Court ruled consistently with *Adjani* in its application of the plain view exception.

The government's retention of StarTests' digital files is also substantially similar to the *Giberson* case. Explicitly rejecting considerations of quantity or format, *Giberson* indicates that the government's discovery of other players' drug use while searching through the large database in an authorized search should not be suppressed. As long as the FBI did not initiate a new, unauthorized search, the FBI committed no violation in discovering other players' drug use in the course of its search. No distinction has been made between printing pornographic images encountered during a search for evidence of fake I.D. cards and retaining information of positive drug results while searching for evidence of drug use by five specific CFL players.

The District Court correctly determined the government's search complied with the elements of the plain view exception, and the government lawfully retained copies of the digital evidence. Because the District Court correctly found that the government's search complied with the elements of the plain view exception, the Fourteenth Circuit should have affirmed the

District's determination on this issue. Unlike the officers from *Carey*, *Miranda*, or *Hicks*, the FBI did not commence a new search, separate and apart from its search for evidence of the five players' drug use. Because CFL and StarTests cannot demonstrate such a search, the District Court was correct to apply the plain view exception and properly denied the plaintiffs' 41(g) motion.

The Fourteenth Circuit, however, reversed the District Court's decision after rejecting the plain view exception. Concerned with the quantity of information stored in digital files, and the fact that the digital data retained by the government necessarily included data of players other than the five in question, the Fourteenth purports to follow the Ninth Circuit in excluding plain view application from digital cases. Yet case law indicates that where an item seized happens to contain other incriminating information not covered by the terms of the warrant, such integration does not compel suppression of the evidence. *United States v. Beusch*, 596 F.2d 871, 877 (9th Cir. Cal. 1979). In fact, the court in *Beusch* "refused to impose the burden of segregation on police," opting instead for broader seizure powers. *Id.* at 876. Furthermore, as *Giberson* makes clear, quantity and integration of data are not valid considerations for Fourth Amendment applications. *Giberson*, 527 F.3d 882, 888.

Despite a myriad of contrary cases in circuits where the issue had arisen, the Fourteenth Circuit defied precedent and excluded the plain-view doctrine from cases involving digital evidence. Instead, the Fourteenth Circuit purported to follow the Ninth Circuit in applying a new approach to digital search and seizure, endorsing the method from *Comprehensive Drug Testing*. In this 2009 case, the Ninth Circuit abandoned the plain view exception to digital evidence, and devised a new system to replace it. *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1006-1007 (9th Cir. Cal. 2009). Citing its concern for the quantity of data that can be stored

digitally, the Ninth Circuit determined that the government should “forswear reliance on the plain view doctrine or any similar doctrine that would allow it to retain data to which it has gained access only because it was required to segregate seizable from non-seizable data.” *Id.* at 998. When the government refuses to waive plain view, said the Ninth Circuit, then the magistrate judge should order “that the seizable and non-seizable data be separated by an independent third party under the supervision of the court,” or else deny the warrant altogether. *Id.* Even after acknowledging the legitimate need by government to “scoop up large quantities of data and sift through it carefully for concealed or disguised pieces of evidence,” *id.* at 1004, the Ninth Circuit declared that the only search protocol that may be authorized (regarding the ten players under investigation in *Comprehensive Drug Testing*) was a protocol designed to discover data “pertaining to those ten names only, not to others, and not those pertaining to other illegality.” *Id.* at 999.

Voicing his strong dissent, Circuit Judge Callahan criticized the majority in *Comprehensive Drug Testing* as too radical and inconsistent with precedent. *Id.* at 1013. Instead, Judge Callahan argued that courts should adhere to the plain view exception, and that if adjustments were required, such adjustments in the law should come from tested, incremental adjudication. *Id.*

The majority essentially jettisons the plain view doctrine in digital evidence cases, requiring that magistrate judges insist that the government waive reliance upon the plain view doctrine in digital evidence cases. It does so, however, without explaining why our case law or the Supreme Court's case law dictate or suggest that the plain view doctrine should be entirely abandoned in digital evidence cases. Instead of tailoring its analysis of the plain view doctrine to the facts of this case, the majority takes the bold step of casting that doctrine aside. Rather than adopting this efficient but overbroad approach, the prudent course would be to allow the contours of the plain view doctrine to develop incrementally through the normal course of fact-based case adjudication. A measured approach based on the facts of a particular case is especially warranted in the case of computer-related technology, which is constantly and quickly evolving. Accordingly, I cannot join in the majority's approach regarding application of the plain view doctrine to digital evidence cases.

*Id.*

Judge Callahan went on to discuss the majority's lack of consideration for the practical consequences of its ruling:

Moreover, the majority offers no support for its protocol requiring the segregation of computer data by specialized personnel or an independent third party. Setting aside the omission of supporting legal authority, this new *ex ante* restriction on law enforcement investigations also raises practical, cost-related concerns. With respect to using an in-house computer specialist to segregate data, the majority's guideline essentially requires that law enforcement agencies keep a "walled-off," non-investigatory computer specialist on staff for use in searches of digital evidence. To comply, an agency would have to expand its personnel, likely at a significant cost, to include both computer specialists who could segregate data and forensic computer specialists who could assist in the subsequent investigation. The alternative would be to use an independent third party consultant, which no doubt carries its own significant expense. Both of these options would force law enforcement agencies to incur great expense, perhaps a crushing expense for smaller police departments that already face tremendous budget pressures.

*Id.*

Just as the majority in *Comprehensive Drug Testing* failed to consider the practical costs and feasibilities of its ruling, the Fourteenth Circuit similarly overlooked these issues. Caught up in the Ninth Circuit's warning against "seizing the haystack to look for the needle" the Fourteenth Circuit's decision discredits existing case law, supplanting a legitimate need for balance with a bright-line rule. This heavy-handed approach distorts and discredits the balance that develops over decades of consideration and evolution in the courtroom.

As discussed above, the majority of case law on this issue (including from the Ninth Circuit prior to 2009) indicates that the plain view exception is readily applicable to digital evidence. Thus, Respondents CFL and StarTests ask the Supreme Court *not* to resolve a circuit split on the issue, but rather to apply the rule from a single case, still in its infancy and untested by subsequent case law, to all the land. It does so despite a cautionary and strongly reasoned dissent from the very case it relies upon, and in the face of volumes of contrary precedent. As dangerous as Judge Callahan deems the drastic amendment to search and seizure protocol for his circuit, it would be far worse for the Supreme Court to apply this untested approach to all the land.

Because the District Court of Wythe properly applied the plain view exception to the digital evidence in this case, and because the FBI complied with all three prongs of the rule, the Fourteenth Circuit's decision should be reversed. The digital evidence retained by the government was obtained during lawful search and seizure, and there is no evidence to support any separate, unauthorized search by the government. As such, the District Court's decision on this issue should be reinstated.

**III. BECAUSE THE WARRANT IN QUESTION WAS MADE TO GUIDE THE SEARCH OF THOUSANDS OF COMPUTER DOCUMENTS THAT WERE HIDDEN, ENCRYPTED, AND DISTRIBUTED OVER SEVERAL COMPUTER SYSTEMS, AND BECAUSE THE SAME WARRANT PROVIDED ENOUGH INFORMATION TO GUIDE OFFICERS IN THEIR SEARCH, THE WARRANT'S AUTHORIZATION ALLOWING OFFICERS TO SEIZE MATERIALS FOR LATER SEARCH WITH BETTER TECHNOLOGY CAPABLE OF ASCERTAINING THE NECESSARY INFORMATION DID NOT VIOLATE THE TENETS OF THE FOURTH AMENDMENT'S REQUIREMENT OF PARTICULARITY.**

The Fourth Amendment makes clear that a warrant issued by a court must “particularly describ[e] the place to be searched, and the persons or things to be seized.” U.S. CONST. amend. IV. Specifically, courts are concerned with the right of the government to issue warrants so general and broad that they would “authorize the wholesale rummaging through a person's property in search of contraband or evidence.” *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. Me. 1999), *People v. Gutierrez*, 2009 Colo. LEXIS 1160, 35-36 (Colo. 2009)(there is a need for a warrant to have “probable cause, specificity...and overall reasonableness” and to not allow officers to simply engage in a rummaging expedition). A warrant must have enough information that the officers have a guide for their search, and it must also be specific enough to prevent the seizure of items not meant to be taken. *Upham*, 168 F.3d at 535. At the same time, warrants need not necessarily describe *how* items may be searched or seized and rarely do so. *Id.* at 537. The warrant must simply address “*what* may be searched or seized.” *Id.*

With these considerations in mind, the United States Court of Appeals for the First Circuit found that, although the warrant had authorized the seemingly broad search of “[a]ny and all computer software and hardware, . . . computer disks, disk drives, which then resulted in an off-site search of that equipment, such an authorization was permissible as the “narrowest definable search and seizure reasonably likely to obtain the images” the officers were seeking. *Id.* at 535. The court, however, noted that “if the images themselves could have been easily obtained through an on-site inspection, there might have been no justification for allowing the seizure of *all* computer equipment, a category potentially including equipment that contained no images and had no connection to the crime.” *Id.* But even with this in mind, the court made an additional note that such an extensive on-site search is difficult and, at least in the instant matter, impracticable. *Id.*

In fact, it is possible that some courts would even allow for the removal of items that have not been listed by the court in the warrant “merely in the reasonable hope that a search of those items later on will lead to recovery of the items that are named.” *Id.* at 536, *United States v. Hargus*, 128 F.3d 1358, 1363 (10th Cir. Okla. 1997)(“search is not invalidated merely because some things are seized that are not stated in the warrant”), *United States v. Schandl*, 947 F.2d 462, 465 (11th Cir. Fla. 1991)(“ seizure of items not covered by a warrant does not automatically invalidate an otherwise valid search”), *United States v. Johnson*, 709 F.2d 515, 516 (8th Cir. Minn. 1983)(it is not unreasonable to seize and remove a container that could hold or contain the evidence sought under the warrant), *United States v. Shilling*, 826 F.2d 1365, 1370 (4th Cir. Va. 1987)(seizure must be “prompted by legitimate practical concerns, rather than by an intent to engage in a fishing expedition). The particularity requirement is offended only when the officers who are conducting the search *grossly* exceed their authorization when

seizing evidence. *Hargus*, 128 F.3d at 1363. For example, the U.S. Court of Appeals for the Tenth Circuit found that officers did not grossly violate the bounds of a search warrant when they seized and removed filing cabinets containing the records they sought after determining that an on-site search would be “impractical and unduly time-consuming.” *Id.* This was true even though the cabinets also contained “unopened mail, office supplies, an answering machine, camera, birthday cards, tape measure, right-of-way papers, horse and cattle papers, and life insurance policies” that were not included in the scope of the warrant. *Id.*

In fact, in some cases, it might not only be impractical but more intrusive to a person’s rights to actually conduct the search of pertinent materials onsite. *Schandl*, 947 F.2d at 465-466. For instance, in the case of crimes such as tax evasion or failure to file taxes, the process of finding information requires a “careful analysis and synthesis of a large number of documents.” *Id.* Conducting such a process onsite could be disruptive – so disruptive that it would actually aggravate the already intrusive nature of the search. *Id.*

The United States District Court for the district of Maine found that too high a standard for particularity in a search warrant for computers will not only cause problems with the officers who must have some latitude in executing them but will confuse the judges who have no background that would enable them to determine what specific kind of computer search is appropriate in which situation. *United States v. Farlow*, 2009 U.S. Dist. LEXIS 112623, \*14-21 (D. Me. 2009), *Shilling*, 826 F.2d at 1369 (“the specificity required for a warrant varies with the circumstances within a ‘practical margin of flexibility’”), *United States v. Gleich*, 2003 U.S. Dist. LEXIS 21834 (D.N.D. 2003)(a warrant is meant to be practically effective not highly technical; the warrant need be only as “specific as the circumstances and nature of activity under investigation permit”). The standard must be broader. *Farlow*, 2009 U.S. Dist. LEXIS 112623

at \*14-\*21. However, despite this need for latitude, the courts must be careful not to allow for overreaching that could allow officers the right to seize items that would otherwise not be appropriate to seize. *Id.* at \*12.

Under this standard, the Court found adequate a warrant that allowed police officers to search all of a suspect's "[c]omputers and computer equipment...electronic data storage devices...software, and written materials relating to the operation of the computer." *Id.* at \*4. Such an allowance included the right to inspect all of the suspect's account names, screen names, and even passwords. *Id.* The warrant indicated that the search was intended to be limited to the crimes under investigation but still allowed an extensive search into internet use, electronic communication, and other personal applications that could store information well beyond the limits of the warrant's intended purpose. *Id.* at \*4-\*5. Because the warrant clearly delineated the specific crimes for which information could be sought, it was not so general as to cause the overreaching the Fourth Amendment tries to prevent. *Id.* at \*13-\*14.

Courts also must ensure a warrant is based on an appropriately specific and accurate affidavit. *Gutierrez*, 2009 Colo. LEXIS at 35. Although a magistrate's determination of probable cause based on the affidavit is given deference, it is not beyond question. *Id.* The Colorado Supreme Court found a warrant lacking when it allowed officers to perform an "extraordinarily wide-sweeping" "exploratory search" of a tax preparation company in the hopes of finding information related illegal immigrants when probable cause was established only as to one, specific immigrant who had used the service. *Id.* at 3. The police used a general affidavit that failed to make any link between the service and other illegal immigrants in order to secure permission to collect two years of tax returns from the service and rummage through those returns looking for other potential crimes. *Id.* at 11-13. Based on this wholly unabated

search, the officers did in fact uncover other illegal immigrants, one of whom was charged with identity theft and criminal impersonation. *Id.* at 3. But the court found that such an affidavit simply could not have provided the magistrate with any substantial reason to “believe that ‘most or all’ of the files would contain evidence of crime.” *Id.* at 47.

The U.S. Court of Appeals for the Ninth Circuit, however, has pushed for a much higher standard in order to avoid transforming every seemingly narrow search into something far more general – a standard meant to prevent overreaching. *Comprehensive Drug Testing, Inc.*, 579 F.3d at 998-1000. According to the Ninth Circuit, a warrant should include some protocol that can ensure information sought matches the information described in the warrant. *Id.* at 1000, *United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. Cal. 1982)(“all items in a set of files may be inspected during a search, provided that sufficiently specific guidelines for identifying the documents sought are provided in the search warrant and are followed by the officers conducting the search”). In other words, the information obtained should have been so obtained because there was probable cause to do so. *Comprehensive*, 579 F.3d at 1000. The court, however, does recognize that, especially when it comes to electronic files, some non-relevant materials might be intermingled with those named in the warrant. In such a case, the magistrate issuing the warrant should appoint special computer personnel who can sort through the information to determine what is relevant and what must be destroyed or returned. *Id.* “[O]nly those personnel may examine and segregate the data” and may not relay any information to government officials that falls outside of the scope of the warrant. *Id.* If those seeking the warrant should refuse such an inclusion, no warrant should issue at all. *Id.* at 998. Furthermore, the government may not copy or retain any unrelated information and must even report the results of its search, both as to the relevant and irrelevant data obtained. *Id.* at 1000-1001. And prior to obtaining the warrant, the

government must disclose the “actual degree” of risk that materials might be intermingled, which could lead to the “concealment and destruction” of evidence. *Id.* at 998.

In its holding, the court also specifically rejected the argument that latitude should be given for a broader search in regard to computer equipment because files can be disguised, erased, hidden, or even destroyed if “certain procedures are not scrupulously followed.” *Id.* at 995. Even in such a case, the magistrate issuing the warrant should require that no materials be removed from the search site if it “c[ould] be searched on-site in a reasonable amount of time and without jeopardizing the ability the preserve the data,” *id.*, simply because the government has “sophisticated hashing tools at its disposal that allow the identification of well-known illegal files...without actually opening the files themselves.” *Id.* at 999. Moreover, even if such information is removed, once the government discovers that such it is not in fact covered by the warrant, it must be returned in, at most, 60 days. *Id.* at 996.

But although its reasoning appears sound, the court’s decision is skewed by the egregiousness of the facts of the case. Pursuant to the warrant described in the case, officers failed to follow the mandates of the warrant, securing and reviewing the files for hundreds of players in the League, as opposed to the 10 in question. *Id.* at 993-994. Moreover, in the process of their search, the officers also “completely ignored” the prescribed screening process and refused the help of someone who could have narrowed the officers’ search results to just the players in question. *Id.* at 996. In fact, despite the pleas of the test facility’s attorney, the case agent took it upon himself to review the information seized from the computers at the facility and use that information to secure another warrant to pursue other players whose information was incriminating, as those other players had not been mentioned in the original warrant. *Id.* at 997. Moreover, there was “no forensic lab analysis, no defusing of booby traps, no decryption, no

cracking of passwords and certainly no effort by a dedicated computer specialist to separate data for which the government had probable cause from everything else.” *Id.* at 999. Such action simply “demonstrated a callous disregard for the rights of those persons.” *Id.*

To address the problem inherent with intermingled files, the U.S. Court of Appeals for the Ninth Circuit suggests that officers who have obtained information outside of the bounds of the warrant “avoid violating *fourth amendment* rights by sealing and holding the documents pending approval by a magistrate of a further search.” *Tamura*, 694 F.2d at 595-596. Materials may be moved under the direction and supervision of the magistrate when it would be unworkable to sort the materials on-site. *Id.* at 596. However, even in the event that unrelated materials are swept into the search, such a sweep does not justify the return of documents obtained legally and soundly via the same warrant. *Id.* at 597.

As such, based on the foregoing case law, a magistrate may issue a warrant that allows officers to remove evidence from the site of investigation when an onsite search is impracticable or unreasonable. Such a warrant, however, must provide clear directions that create a guide for investigating officers to ensure that officers cannot use any ambiguous to parameters engage in a rummaging or fishing expedition intended only to uncover unrelated materials.

Thus, the warrant issued by Magistrate Leon did not offend the particularity requirement of the Fourth Amendment because, as in *Upham*, the StarTests material to be searched was especially extensive. Specifically, the search involved thousands of files that had amassed over the course of four years – a search that ultimately took weeks to conduct – making it impracticable and almost impossible to search such files while on site. In fact, a computer forensic agent onsite had examined the materials and recommended they be seized or copied for further review. Moreover, as suggested in *Schandl*, such an extensive onsite search could have

actually been more intrusive than the simple removal of information for future searches; because StarTests likely continued to operate its business during the course the investigation, a continued presence of officers at StarTests' facilities for weeks would clearly be an intrusion that violated its Fourth Amendment rights more than a simple removal of the items in question. Additionally, the files were not kept in a single, easily sorted database but were, instead, maintained in a "computer-hopping" procedure whereby StarTests separated the data into three systems, many with encryption and some deceptively hidden or mislabeled on various other drives. Such a search required special technical knowledge and special software not possessed by the officers onsite. Even a computer forensics agent who was onsite recommended the removal of the files due to a lack of ability to efficiently and effectively ascertain the information needed.

The warrant also provided enough information to ensure agents had the appropriate guidance. Specifically, as per *Upham*, the warrant indicated what was to be searched and seized: "all computer records, files, and equipment" related to the agents' search, and although this seems like a fairly broad directive, *Upham* allows such breadth in description because it was the most narrowly defined description that would still allow agents to search and seize the materials necessary to their investigation. Had the officers been directed to certain computers or certain equipment, inadvertently leaving out others not known to be a part of StarTests' computer-hopping system, they might not have been able to secure enough information to indict the players originally suspected of illegal drug use. Moreover, the warrant specifically indicated that the information was to be limited to the records and information "reasonably related to the investigation into the five named players' illegal steroid use." *Farlow* makes clear that, as long as this delineation of specific crimes is in place, the otherwise extensive search of the computer systems was justified by the facts of the case.

Those who adhere strongly to the strict standards set forth in the *Comprehensive* decision might argue this position for two reasons. First, such proponents might suggest that the computer forensics agent onsite in the instant matter was not an appropriate person to make the determination that items be removed for later inspection because the agent was not appointed specially for that purpose. The agent in this case, however, did not need to be specially appointed, as the warrant required only a cursory inspection by “trained personnel.” Unlike the warrant in *Comprehensive*, there was no special mandate that the agent be designated for that special purpose. Followers of *Comprehensive* also might argue that it was the Magistrate’s responsibility to put in place a searching protocol that would better guide the agents’ search and lessen the possibility of a general rummaging through StarTests’ files, but such a standard would undoubtedly impede the agents’ ability to collect the information sought even as to the five players named in the warrant. It likely would have been impossible to develop a search protocol that could anticipate hidden and misnamed files, a three-part computer system, and a need for special software that could decode the elaborate system developed specifically for secrecy and confidentiality. Moreover, as indicated in *Farlow*, judges do not often have the technological background that would be required to put such a system in place.

As such, the need for an extensive, time-consuming search into thousands of documents obscured by a complicated three-computer system justified the warrant’s broad language permitting the removal of the information from the StarTests’ laboratory. Additionally, although somewhat broad, the warrant contained enough information to guide officers in their search which is all that is necessary to satisfy the mandates of the Fourth Amendment.

## CONCLUSION

This Court should reverse the Fourteenth Circuit’s decision and deny Respondents’ 41(g) motion. In doing so, this Court is presented the opportunity to avert serious damage to the future and efficiency of law enforcement by protecting the ability of law enforcement to effectively prosecute crime. The Colonial Football League lacks standing to bring its vicarious 41(g) claim because the CFL was not itself a victim of a search. Furthermore, this Court should reestablish the traditional application of the plain view doctrine to digital evidence and find that the evidence retained by the government was obtained by proper means within the ambit of the plain view rule. Finally, case law makes clear that a federal magistrate does not offend the Fourth Amendment’s mandate of particularity by issuing a warrant that grants officers some latitude in conducting a search, including the right to seize computer equipment for a later search when the necessary information cannot be obtained during an onsite investigation. Such warrants must simply guide the officers’ search – not specifically describe every item sought.

Therefore, in light of the foregoing, this Court should reverse the Fourteenth Circuit’s decision and affirm the District Court of Wythe’s denial of Respondents’ Motion under Fed. R. Crim. P. 41(g).

## CERTIFICATE OF SERVICE

The foregoing brief was served upon Attorney for the Respondent on the 12<sup>th</sup> day of January, 2010, at the following address:

Respondent’s Attorney, Esq.  
William and Mary School of Law  
613 South Henry St.  
Williamsburg, VA 23185

Dated: January 12, 2010

ID No. \_\_\_\_\_ **Team No. 7** \_\_\_\_\_