

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 WRIT OF CERTIORARI TO THE
UNITED STATES COURT OF APPEALS
FOR THE FOURTEENTH CIRCUIT***

BRIEF FOR PETITIONER

Team 1
Counsel for the Petitioner

January 13, 2010

COLLEGE OF WILLIAM AND MARY
SPONG MOOT COURT COMPETITION

TABLE OF CONTENTS

	<u>Page</u>
<u>TABLE OF CONTENTS</u>	1
<u>TABLE OF AUTHORITIES</u>	3
<u>CONSTITUTIONAL PROVISIONS AND STATUTES INVOLVED</u>	6
<u>QUESTIONS PRESENTED</u>	7
<u>OPINIONS BELOW</u>	8
<u>STATEMENT OF THE CASE</u>	9
<u>SUMMARY OF THE ARGUMENT</u>	12
<u>ARGUMENT</u>	14
I. THE FOURTEENTH CIRCUIT ERRED IN FINDING THAT THE CFL HAS STANDING TO SUE ON BEHALF OF ITS PLAYERS FOR THE RETURN OF ILLEGALLY SEIZED PROPERTY UNDER FED. R. CRIM. P. 41(G)	14
A. <u>The CFL Is Not A Victim of the Government’s Search</u>	14
B. <u>The CFL Lacks Associational Standing to Sue on Behalf of Its Members</u>	17
C. <u>Associational Standing is Inapplicable to Fourth Amendment Cases</u>	19
II. THE FOURTEENTH CIRCUIT ERRED IN DETERMINING THAT THE STARTESTS WARRANT WAS NOT SUFFICIENTLY PARTICULAR	20
A. <u>The StarTests Warrant Met The Particularity Requirements Set Forth By The Supreme Court And A Majority Of Federal Circuit Courts</u>	20
B. <u>The Fourteenth Circuit Incorrectly Applied <i>Tamura</i> To A Single File Of Information</u>	24
C. <u>The Special Warrant Procedures For Computer Searches Set Forth in <i>Comprehensive Drug Testing</i> Are Neither Required By Nor Advisable Under The Fourth Amendment</u>	27
D. <u>The <i>Comprehensive Drug Testing</i> Warrant Procedures Are Incompatible With Recent Amendments To Rule 41(g)</u>	31
III. THE FOURTEENTH CIRCUIT ERRED BY REFUSING TO EXTEND THE PLAIN VIEW DOCTRINE TO DIGITAL EVIDENCE SEARCHES	34

A. This Search Satisfies The Traditional Plain View Requirement34

B. Heightened Fourth Amendment Protections Should Not Be Technology-Specific37

IV. THE GOVERNMENT’S CONDUCT WAS NOT SO EGREGIOUS AS TO REQUIRE A RETURN OF SEIZED PROPERTY UNDER RULE 41(G).....40

CONCLUSION44

TABLE OF AUTHORITIES

Constitutional Provisions

U.S. CONST. AMEND. IV *passim*

Cases

United States Supreme Court

<i>Coolidge v. New Hampshire</i> , 403 U.S. 443 (1971)	20, 34
<i>Groh v. Ramirez</i> , 540 U.S. 551 (2004)	20
<i>Horton v. California</i> , 496 U.S. 128 (1990)	34, 35, 37
<i>Hunt v. Washington State Apple Advertising Comm'n</i> , 432 U.S. 333 (1977).....	17
<i>Jones v. United States</i> , 362 U.S. 257 (1960).....	14-15
<i>Minnesota v. Carter</i> , 525 U.S. 83 (1998).....	17
<i>Minnesota v. Olson</i> , 495 U.S. 91 (1990).....	15
<i>Pennell v. City of San Jose</i> , 485 U.S. 1 (1988)	17
<i>Rakas v. Illinois</i> , 439 U.S. 128 (1978).....	14, 15, 18, 19
<i>Rawlings v. Kentucky</i> , 448 U.S. 98 (1980).....	14
<i>United Food & Commercial Workers Union Local 751 v. Brown Group</i> , 517 U.S. 544 (1996)..	18
<i>United States v. Salvucci</i> , 448 U.S. 83 (1980).....	15
<i>Valley Forge Christ. Coll. v. Ams. United for Separation of Church and State, Inc.</i> , 454 U.S. 464 (1982).....	9,10
<i>Warth v. Seldin</i> , 422 U.S. 490 (1975).....	17, 18, 19

United States Courts of Appeal

In re Impounded Case, 840 F.2d 196 (3d Cir. 1988).....

21

<i>Ramsden v. United States</i> , 2 F.3d 322 (9th Cir. 1993).....	40
<i>Richey v. Smith</i> , 515 F.2d 1239 (5th Cir. 1975).....	40, 41
<i>Search of Kitty’s East v. United States</i> , 905 F.2d 1367 (10th Cir. 1975)	22, 42
<i>United States v. Adjani</i> , 452 F.3d 1140 (9th Cir. 2006).....	<i>passim</i>
<i>United States v. Beusch</i> , 596 F.2d 871 (9th Cir. 1979).....	25, 26, 27
<i>United States v. Brooks</i> , 427 F.3d 1246 (10th Cir. 2005).....	21, 27, 30
<i>United States v. Burzynski Cancer Research Institute</i> , 819 F.2d 1301 (5th Cir. 1987).....	15
<i>United States v. Carey</i> , 172 F.3d 1268 (10th Cir. 1999)	<i>passim</i>
<i>United States v. Comprehensive Drug Testing</i> , 579 F.3d 989 (9th Cir. 2009).....	<i>passim</i>
<i>United States v. Fitzen</i> , 80 F.3d 387, 388 (9th Cir. 1996).....	42-43
<i>United States v. Giberson</i> , 527 F.3d 882 (9th Cir. 2008)	29, 36-39
<i>United States v. Hall</i> , 142 F.3d 988 (7th Cir. 2006).....	21-22
<i>United States v. Hill</i> , 459 F.3d 966 (9th Cir. 2006).....	23, 31
<i>United States v. Leary</i> , 846 F.2d 592 (10th Cir. 1988).....	21, 22
<i>United States v. McConnell</i> , 400 F.2d 347 (5th Cir. 1974).....	15
<i>United States v. Meek</i> , 366 F.3d 705 (9th Cir. 2004).....	21, 24
<i>United States v. Raney</i> , 342 F.3d 551 (7th Cir. 2003)	35
<i>United States v. Reyes</i> , 798 F.2d 380 (10th Cir. 1986).....	22
<i>United States v. Taketa</i> , 923 F.3d 665 (9th Cir. 1991)	15
<i>United States v. Tamura</i> , 694 F.3d 184 (9th Cir. 1982).....	12, 24-26
<i>United States v. Walser</i> , 275 F.3d 981 (10th Cir. 2001).....	39
<i>United States v. Wong</i> , 334 F.3d 831 (9th Cir. 2003).....	35, 37-38

United States District Courts

United States v. Gray, 78 F.Supp.2d 524 (E.D. Va. 1999) 27-28, 35

United States v. Hill, 322 F.Supp.2d 1081 (C.D. Ca. 2004)..... 28-29

United States v. Vilar, No. 05-CR-621, 2007 WL 1075041 (S.D.N.Y. 2007) 27-29

Rules and Statutory Provisions

FED. R. CRIM. P. 41(g) *passim*

Secondary Sources

Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 569 (2005) ...27

CONSTITUTIONAL PROVISIONS AND STATUTES INVOLVED

U.S CONST. AMEND. IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon . . . particularly describing the place to be searched, and the . . . things to be seized.

QUESTIONS PRESENTED

- I. Does an organization that contracts with a third party to perform drug testing and store the results have standing to sue on behalf of its members for the return of records illegally seized from the third party under Fed. R. Crim. P. 41(g)?
- II. Are there any circumstances in which federal magistrates may issue warrants authorizing the government to seize all computer equipment and files for later sorting, or must the particularity requirement be heightened in the digital evidence context, as per the guidelines announced in the Fourteenth Circuit below and in *United States v. Comprehensive Drug Testing*, 579 F.3d 989 (9th Cir. 2009)?
- III. Should the “plain view” exception to the Fourth Amendment’s warrant requirement be completely disposed of in digital searches and seizures?

OPINIONS BELOW

The United States District Court for the District of Wythe held that although the CFL Plaintiffs had standing to bring a Fed R. Crim P. 41(g) motion for return of property, that property was properly seized under the plain view doctrine and pursuant to a valid warrant. As the search was not illegal, the district court held that the Plaintiffs had no right to have the information returned under Fed. R. Crim. P. 41(g). (R at 2.)

The U.S. Court of Appeals for the Fourteenth Circuit affirmed the decision of the district court with respect to the standing of the CFL Plaintiff, but reversed the district court's conclusions regarding the legality of the search. Citing the unique properties of computers, the court of appeals eschewed the doctrine in digital evidence cases altogether. (R. at 13.) Instead, it hewed closely to the Ninth Circuit's *Comprehensive Drug Testing* decision, adopting the same five rules magistrates must follow in digital evidence cases:

- (1) Magistrates should insist that the government waive reliance upon the plain view doctrine.
- (2) Segregation and redaction of the computer evidence must be either done by specialized personnel or an independent third party. If done by government personnel, that personnel must agree not to disclose any information other than that which is the target of the warrant.
- (3) Warrants must disclose the actual risks of destruction or concealment of information, as well as prior efforts to seize that information in other courts.
- (4) The government's search protocol must be designed to uncover only the information for which it has probable cause, and only noncomputer personnel agents may examine that information.
- (5) The government must destroy, or, if the recipient may lawfully possess it, return nonresponsive data, at all times keeping the court informed of its progress. (R. at 17.)

STATEMENT OF THE CASE

Statement of the Facts

In 2003, the Colonial Football League (“CFL”) began requiring its franchises to submit players for drug tests. (R. at 1.) It later hired StarTests, Inc. (“StarTests”), an independent drug testing business, to conduct the tests. (*Id.*) CFL and StarTests (collectively “Plaintiffs”) informed the players that the tests were to determine the frequency of illegal steroid use among the football players as a whole rather than that of specific players, and that as such, names and results would remain anonymous. (*Id.*) Test results were stored at StarTests’ facility with only the name and percentage of players using steroids released to CFL. (*Id.*)

In July 2008, the Federal Bureau of Investigation (FBI) began an investigation of the use of steroids in professional sports. (R at 7.) In the process of this investigation, it discovered in particular that five players had been engaging in illegal steroid use. (*Id.*) It applied for a warrant to seize material regarding this investigation from the StarTests facility, located in Millersville, Wythe. (R at 1.) The supporting affidavit for the warrant included a request for permission to seize urine samples and documents, but also “all computer records, files, and equipment” related to the StarTests tests of the players. (R at 1-2.) The affidavit noted that all equipment and files would need to be seized and reviewed at a later date because time constraints would not permit a search of such massive amounts of files on-site, some of the files may be deceptively labeled, and software needed to access encrypted files might be required not available on StarTests’ computers (R at 2.) Magistrate Judge Leon issued the warrant, permitting the FBI to search “computer equipment, storage devices, and – where an on-site search would be impracticable – seizure of either a copy of all data or the computer equipment itself.” (*Id.*) However, the warrant required “law enforcement personnel trained in searching and seizing computer data” to determine whether a computer needed to be seized.” (*Id.*) The warrant also required that if a

computer were seized, “appropriately trained personnel” were to review the data, retaining information authorized by the warrant and returning the rest. Further, Judge Leon restricted the search and seizure to information “reasonably related to the investigation into the five named players’ illegal steroid use.” (*Id.*)

The FBI executed this warrant November 1, 2008. When agents asked about the location of the CFL drug test results, StarTests personnel informed them most of the computers on the facility contained at least one database on the CFL drugs tests. (*Id.*) Additionally, many of those files were encrypted or hidden on H or S-drives. (*Id.*) Thus, the head agent ordered the copying or seizure of all computer equipment depending on how easily the equipment could be extracted. (*Id.*)

The equipment, documents and urine samples were all taken to the FBI office in Wythe City, where computer forensics agents viewed the databases and matched the test results to the players. (*Id.*) In the process of doing so, forensics agents came upon test results of other players revealing positive tests for a variety of non-steroid illegal drugs including cocaine, marijuana, and a variety of hallucinogens. (*Id.*) On the basis of this information, the FBI decided to expand the investigation to include all illegal drug possession and sale within professional football. (*Id.*) It proceeded to copy and inventory the computer hard drives and returned unneeded equipment to StarTests. (*Id.*) Plaintiffs StarTests and CFL then filed a motion for the return of the copied electronic materials under Fed. R. Crim. P. 41(g). (*Id.*)

Procedural History

Plaintiffs filed motion in the United States District Court for the District of Wythe for return of the copied materials under Fed. R. Crim. P. 41(g), alleging that the warrant was not

sufficiently particular, or alternatively, that the seizure was outside the scope of the warrant and was thus barred by the Fourth Amendment. (R at 9.) The District Court held that CFL had standing to bring the motion on behalf of its members, but found that the seizure was legal (R at 3). It thus denied Plaintiffs' motion for return of property (R. at 6.)

Plaintiffs appealed the district court's findings with regard to the legality of the search, and the Government appealed the issue of standing. (R. at 9.) The Fourteenth Circuit Court of Appeals affirmed the lower Court's ruling on the issue of standing. (R at 10). Regarding the legality of the search, the Court of Appeals reversed the ruling of the district court, electing instead to adopt a heightened standard for computer searches and seizures (*supra* at 2). Petitioner, the United States of America, now appeals this ruling.

SUMMARY OF THE ARGUMENT

The Fourteenth Circuit made four critical errors. First, it incorrectly found that Respondent CFL had standing to sue on behalf of its players for the return of illegally seized property under Fed. R. Crim. P. 41(g). In order to claim standing, CFL would have to have a property interest in the area containing the databases. Furthermore, CFL fails to meet the test that this Court has set out for associational standing to sue on behalf of an organization's members because the players themselves lack a property interest in the databases, protection of steroid abusing athletes runs counter to the organization's purpose, and the inquiry involved would require the participation of its members. Additionally, associational standing is inapplicable within the context of the Fourth Amendment. Traditional standing doctrine allows associational standing because it does not require an individual to assert that his rights have been violated. Fourth Amendment law, on the other hand, requires a personal assertion of one's own rights.

Second, the Fourteenth Circuit wrongly concluded that the search warrant issued in this case was overbroad. Under the precedents of this Court and a majority of federal courts, the warrant issued in this case is sufficiently particular, because the face of the warrant expressly limited the search and seizure to evidence reasonably related to a crime for which probable cause existed. Furthermore, the fact that the computer files seized contained illegal drug results relating to the investigated players as well as third parties for which no probable cause existed did not trigger the special disambiguation procedures described in *United States v. Tamura*, because all the data searched was contained within the same file. In addition, the Fourteenth Circuit's adoption of a heightened particularity requirement above and beyond the standard set out by this Court is unsupported by precedent and practically unwise, because of the various and unpredictable concealment measures at issue in this case and employed by computer users

generally. Finally, the heightened standard adopted by the Fourteenth Circuit is at odds with recent amendments to Fed. R. Crim. P. 41(g), which recognize the importance of government “overseizure” in electronic data cases.

Third, the Fourteenth Circuit erred by disposing entirely of the plain view doctrine in the context of electronic data searches. Under the precedents of this Court, the search in this case met the requirements of the plain view doctrine. Furthermore, this Court has always held that Fourth Amendment protections should not be technology-specific because heightened requirements for certain types of evidence are not in line with the Fourth Amendment. A heightened plain view standard is also overbroad and places too high of a burden on law enforcement officials, because using a “third party” to separate out relevant data would raise the cost of searches and ultimately be more intrusive.

Finally, the government’s conduct was not so egregious as to merit a return of property under Fed. R. Crim. P. 41(g). Courts interpreting Rule 41(g) have held that a motion under this rule will only succeed when the government has shown a “callous disregard” for the rights of individual victims. Acting pursuant to a search warrant that was later declared invalid, the government did not engage in any deceitful or fraudulent conduct that would meet the standard of callous disregard. As such, regardless of whether the property at issue was indeed illegally seized, the Fourteenth Circuit should not have granted Respondent’s 41(g) motion.

ARGUMENT

I. THE FOURTEENTH CIRCUIT ERRED IN FINDING THAT THE CFL HAS STANDING TO SUE ON BEHALF OF ITS PLAYERS FOR THE RETURN OF ILLEGALLY SEIZED PROPERTY UNDER FED. R. CRIM. P. 41(G)

A. The CFL Is Not A Victim of the Government's Search

The Fourth Amendment standing rule is well settled by this Court. The ability of an individual to claim the protections of the Fourth Amendment depends on whether the person has a legitimate expectation of privacy in the invaded place. *Rakas v. Illinois*, 439 U.S. 128, 143 (1978). This is both a subjective expectation, as well as an expectation that is objectively reasonable. *Id.* at 143 n.12. (“Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.”). Set in the language of Rule 41(g), which requires the movant to be “aggrieved by an unlawful search and seizure of property or by the deprivation of property,” this Court has held that in order to qualify as a such a person, “one must have been a victim of a search and seizure, one against whom the search was directed, as distinguished from one who claims prejudice only through the use of evidence gathered as a consequence of a search or seizure directed at someone else.” *Jones v. United States*, 362 U.S. 257, 261 (1960).

Although this Court has recognized that the capacity to claim the protection of the Fourth Amendment does not depend entirely upon a property right in the invaded place, *Rakas*, 439 U.S. at 143, this Court has also held that it is insufficient to assert standing simply based on an interest in the property seized. *See id.* at 130 (holding that defendant could not contest the search of a glove box in a car he did not own that yielded incriminating evidence which he also did not own). *See also Rawlings v. Kentucky*, 448 U.S. 98, 105 (1980) (holding that defendant did not

have a reasonable expectation of privacy in a purse he did not own because he had no right to exclude others from searching it); *United States v. Salvucci*, 448 U.S. 83 (1980) (holding that defendants had no right to exclude stolen mail seized by police during a search of the apartment rented by one defendant's mother).

Most courts have also required plaintiffs to either be present in or have an uncompromised right of access to in the area the property at issue was seized from. *See United States v. Burzynski Cancer Research Institute*, 819 F.2d 1301 (5th Cir. 1987) (holding that patients had no property interest in the information contained in their medical files, and even if they had that interest, were still required to demonstrate a legitimate expectation of privacy in the business premises the files were seized from). This Court has upheld that model, going so far as to hold that persons who are simply "legitimately on the premises" cannot claim they have a reasonable expectation of privacy against search or seizure. *Rakas*, 439 U.S. at 142-48. Using the same analysis but reaching an opposite result, the Court has justified the reasonable expectations of privacy of overnight guests in a residence that is not their own, because such guests are "much more than just legitimately on the premises." *Minnesota v. Olson*, 495 U.S. 91, 98-99 (1990). *See also Jones*, 362 U.S. at 261 (1960). Conversely, a defendant cannot claim standing if he neither has a cognizable property interest in the place or thing searched, nor was present at the time of the search. *See United States v. McConnell*, 400 F.2d 347 (5th Cir. 1974) (holding that defendant had no reasonable expectation of privacy in a rental car paid for by the defendant to hold against a search for which he was not present); *United States v. Taketa*, 923 F.2d 665 (9th Cir. 1991) (holding that mere access to an office was insufficient to grant a legitimate expectation of privacy to someone who neither was present at the time of the search, nor had a property interest in the items seized).

Furthermore, this Court has also been unwilling to grant Fourth Amendment standing to parties where their primary purpose for being on the premises was for a commercial transaction. *See Minnesota v. Carter*, 525 U.S. 83 (1998). In *Carter*, this Court propounded a four-prong inquiry to determine the reasonableness of a third-party's privacy expectation in another's property. It noted that "property used for commercial purposes is treated differently for Fourth Amendment purposes than residential property," and that expectations of privacy in commercial premises are "different from, and indeed less than, a similar expectation of privacy in an individual's home." *Id.* at 90. The Court in *Carter* ultimately found that the "purely commercial nature of the transaction engaged in" lead to a finding that the defendant there lacked standing to challenge a search under the Fourth Amendment. *Id.* at 91.

The government agents in this case seized three computers from StarTests laboratories, none of which were owned in any part by CFL. Nor was CFL on the premises of the StarTests lab when the seizure of the databases took place. It is unclear from the record whether CFL had a right of access to StarTests labs, but based on the high level of vigilance with which StarTests protected the confidentiality of the records of its other clients, it is unlikely that such was the case. Furthermore, the fact that the nature of its "presence" on StarTests premises was purely a result of a commercial contract with StarTests for drug testing of its players cuts against a finding of the reasonableness of that expectation. This Court has been unwilling to hold that a mere interest in the property seized is sufficient to generate Fourth Amendment standing, and in this case, CFL did not create, store, or guard the records seized by the government. As a result, they were not "a victim of the search, or one against whom a search was directed" for the purposes of Rule 41(g), and therefore had no standing to contest the search of StarTests' lab.

B. The CFL Lacks Associational Standing to Sue on Behalf of Its Members

The Fourteenth Circuit incorrectly found that the CFL had associational standing to sue on behalf of its members. Traditionally, standing requires “actual injury redressable by the court.” *Valley Forge Christian Coll. v. Ams. United for Separation of Church and State, Inc.*, 454 U.S. 464, 472 (1982). The Supreme Court has been clear that generally, only those whose rights are being infringed should assert constitutional challenges. As this Court held in *Singleton v. Wulff*, 428 U.S. 106, 113-114 (1976), “[t]he courts depend on effective advocacy, and therefore should prefer to construe legal rights only when the most effective advocates of those rights are before them. The holders of the rights may have a like preference, to the extent they will be bound by the courts' decisions under the doctrine of stare decisis.”

However, in limited circumstances, this Court has allowed an association to sue on behalf of an individual when it meets the following three requirements: the interest must be one that could be asserted by individual members of the association, it must be germane to the organization's purpose, and must be one that does not require the participation of individual members. *Pennell v. City of San Jose*, 485 U.S. 1, 7 n.3 (1988). Determining whether individual members would have standing is simply a matter of applying the test for standing described in Pt. I.A, *supra*. The court typically holds that the second requirement is met in cases in which the action is unambiguously in the best interest of organization and its members. *Hunt v. Washington State Apple Advertising Comm'n*, 432 U.S. 333 (1977) (upholding standing for an agency representing the interests of apple growers to challenge a statute which made the process of selling apples more expensive). For the third requirement, the court has found associational standing is best suited for cases of injunctive or declaratory relief “because the remedy, if granted, will inure to the benefit of those members of the association actually injured.” *Warth v.*

Seldin, 422 U.S. 490, 515 (1975). The purpose of the first two prongs of this test is to assure that the plaintiff has a sufficiently substantial stake in the outcome of the litigation, whereas the purpose of the third prong rests of policy notions of efficiency and convenience. *United Food & Commercial Workers Union Local 751 v. Brown Group*, 517 U.S. 544, 556 (1996).

CFL fails the requirements for associational standing because individual players would not have standing to bring suit on the matter as they had no legitimate expectations of privacy in the invaded StarTests lab. None of the individuals whose records were seized owned these records (they were the property of StarTests), and neither were any of those individuals on the premises of StarTests when the search was conducted. Furthermore, all of these individuals had voluntarily given urine and blood samples to StarTests to conduct the appropriate testing, which waived their reasonable expectations of privacy in the results of those tests. *See United States v. Comprehensive Drug Testing*, 579 F. 3d 989, 1023 n.20 (9th Cir. 2009) (Ikuta, J., dissenting) (“I am aware of no court which has held that bodily fluids voluntarily given away, and held in possession of a third party, are owned by the donee.”). Additionally, the record does not show the existence of any contract between the players and StarTests or any other understanding between those two parties necessary to prove the players would have standing under *Rakas* and Rule 41(g) to claim violation of their Fourth Amendment rights.

CFL also fails the “germane” prong of the test for associational standing, because the association cannot assure effective advocacy of the relevant issue. In this case, CFL has a conflict of interest in representation. On the one hand, it may to some degree desire to preserve the privacy interests of its players. On the other hand, it is a football league with a strong interest in upholding its public image by discouraging player steroid use. (R at 2.) It is likely that the CFL will shy away from being labeled a zealous advocate of steroid users or an organization that

actively conceals steroid use. This conflict of interest casts serious doubt on its ability to advocate for its players who have willfully violated its rules through the use of illegal substances.

Finally, CFL's suit fails the third prong of the associational standing test because it would require the participation of individual members. Though normally injunctive relief meets the third prong of the test for associational standing, here such relief would be overbroad. The rationale mentioned in *Warth* does not apply in this case, because whatever relief is to be received would have to be tailored to only apply to those players who could demonstrate they had the legitimate expectation of privacy required by *Rakas*. Because the CFL's suit does not meet any prong of the requirement, the lower court's assessment that CFL has associational standing should be overturned.

C. Associational Standing is Inapplicable to Fourth Amendment Cases

The lower court also improperly applied associational standing to the Fourth Amendment inquiry, which uses a different standard. This Court has distinguished between Fourth Amendment rights and other traditional notions of standing, holding that the standing inquiry in the Fourth Amendment context "is more properly placed within the purview of substantive Fourth Amendment law than within that of standing." *Rakas*, 439 U.S. 128, 139 (1978). In *Rakas*, this Court narrowed the definition of those who could claim standing, rejecting a reading that would allow anyone who was injured by the violation, as would have been true in traditional standing jurisprudence, to those who have a legitimate expectation of privacy in the property seized. 439 U.S. 128, 141 (1978). These limitations preclude the application of associational standing to Fourth Amendment cases. This Court has emphasized that only those whose rights have been violated should benefit from Fourth Amendment protections, and due to the strong incentives for individuals to assert these rights themselves, there is no need to permit others to assert such rights for them. *Rakas*, 439 U.S. at 133. Indeed, this Court has never applied

associational standing to a Fourth Amendment case, and has limited its application to contexts which associations traditionally permeate. *See, e.g., Pennell*, 485 U.S. 1 (1988) (upholding the validity of a rent control statute); *Warth*, 422 U.S. 490 (1975) (examining standing in a case involving validity of zoning ordinance).

The case at bar fits this profile. The lower court recognized that if the players wished, they could initiate motions themselves for the return of the property. (R. at 3.) As such, a claim by the CFL of an alleged violation of the players Fourth Amendment rights is precisely the sort of vicarious assertion *Rakas* warned against. Instead, in the Fourth Amendment context, only those who feel their own rights have been infringed are permitted to bring claims based upon the violations. Thus, because the lower court misunderstood this legal standard, it should be reversed.

II. THE FOURTEENTH CIRCUIT ERRED IN DETERMINING THAT THE STARTESTS WARRANT WAS NOT SUFFICIENTLY PARTICULAR

A. The StarTests Warrant Met The Particularity Requirements Set Forth By The Supreme Court And A Majority Of Federal Circuit Courts

The primary rules governing search warrants are well established by Supreme Court jurisprudence. The Fourth Amendment requires that a search warrant describe the things to be seized with sufficient particularity to prevent a general, exploratory rummaging in a person's belongings. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). This requirement ensures that a search is confined in scope to particularly described evidence relating to a specific crime for which there is demonstrated probable cause. *Id.* Beyond its function of limiting police powers, the particularity requirement also “assures the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search. *Groh v. Ramirez*, 540 U.S. 551, 561 (2004).

As a general matter, courts have been willing to invalidate a warrant as overbroad that authorizes the seizure of every record, document, or file in a specified place with no regard to whether the seized materials are connected to criminal activity mentioned in the warrant. *See U.S. v. Leary*, 846 F.2d 592, 602 (10th Cir. 1988) (holding that the broad language of the warrant impermissibly authorized the seizure of “virtually every document one might expect to find in a . . . company’s office” including those with no connection to criminal activity providing the probable cause for the search). In *Leary*, the 10th Circuit considered the validity of a warrant issued to seize a “laundry list” of illegal materials from an export company “in violation of the Arms Export Control Act.” *Id.* at 594. In the context of a search of an export company, the court held the limitations in the warrant to seize materials violating a broad federal statute provided “no limitation at all.” *Id.* at 601.

Consistent with *Leary*, a majority of courts have been willing to uphold warrants under the particularity requirement when the language of the warrant authorizes only the seizure of items relating to a specific crime. *See, e.g., U.S. v. Brooks*, 427 F.3d 1246 (10th Cir. 2005) (upholding warrant for seizure of evidence related to child pornography); *In re Impounded Case*, 840 F.2d 196 (3rd Cir. 1988) (upholding warrant for search of a law office for items relating to crimes of tax evasion and mail fraud); *U.S. v. Hall*, 142 F.3d 988 (7th Cir. 1998) (upholding warrant for search and seizure of computer hardware, disk drives, and programs that are “used or may be used” to depict child pornography); *U.S. v. Meek*, 366 F.3d 705 (9th Cir. 2004) (ruling warrant authorizing search of computer equipment not overbroad because it specifically referred to items related to the sexual exploitation of children). Unlike the warrant in *Leary*, when items listed to be seized are qualified by their connection to a particular crime for which probable cause exists, police officers executing the warrants “are not unguided and free to rummage

through [the victim's] property.” *Hall*, 142 F.3d at 996-97. The Tenth Circuit in *Leary* made clear that the scope of the warrant at issue in that case exceeded probable cause. 846 F.2d at 605.

By and large, federal courts avoid reading language in warrants narrowly because of the uncertainties inherent in modern-day evidence gathering. *See Search of Kitty's East v. United States*, 905 F.2d 1367, 1374 (10th Cir. 1975) (holding that the language in warrants is to be read in a “commonsense fashion,” with a “practical margin of flexibility permitted by the constitutional requirement for particularity in the description of the items to be seized”). In *Kitty's East*, the Tenth Circuit upheld a warrant authorizing the seizure of business records relating to a money laundering scheme as sufficiently particular because the executing officers could not, in compliance with the warrant, “seize any and all business records on Kitty’s premises, but rather were restricted to certain products, certain business or individuals, and certain time periods. *Id.* at 1375. This “commonsense approach” to the particularity requirement stems from the difficulties involved in “describing with exactitude the precise form the records will take.” *United States v. Reyes*, 798 F.2d 380, 383 (10th Cir. 1986). In *Reyes*, the 10th Circuit upheld a police seizure of a cassette tape pursuant to a warrant for drug trafficking “records, ledgers, and writings.” *Id.* at 382. It cited the “age of modern technology and commercial availability of various forms of items” as the justification for reading the warrant broadly. *Id.* at 383. As long as the officers “knew the records they were seeking might be contained on the tape,” it reasoned, such items could be lawfully seized pursuant to the warrant. *Id.*

The concerns of the Tenth Circuit with regard to finding evidence of crime in the age of microchips are especially relevant here. As discussed in Part II.C, *infra*, there are many ways for computer users to hide evidence of criminal activity on computers. As a result, it would be unwise for this Court to follow the Fourteenth Circuit’s heightened standard of particularity in

computer search cases. Instead, it should adhere to the prevailing standards for warrant specificity, which are met by Magistrate Judge Leon's warrant in this case. The government's warrant authorized the FBI to search "computer equipment and storage devices" and to retain copies of that data where on-site searching would be impractical. (R. at 2.) There is nothing illegal, or even uncommon, about warrants authorizing such searches. Furthermore, the warrant on its face restricted the search to information "reasonably related to the investigation into the five named players' illegal steroid use." (R. at 2). This prevented the police from executing an impermissible "general search" under *Coolidge*, and limited them to seizing computer files associated with a crime for which probable cause existed. Thus, the warrant on its face was in line with the particularity requirements of this Court and a majority of the federal circuits.

The Fourteenth Circuit's opinion suggests that allowing such broad language in warrants would delimit searches by giving police "free rein over search protocol that does not meet the constitutional requirement of a narrowly tailored, particular search warrant." (R. at 15). However, aside from the anomalous decision of the Ninth Circuit in *Comprehensive Drug Testing*, discussed in Part II.C, *infra*, broad warrants have traditionally been upheld on various public policy grounds. *See* (Op. at 18. (Oneida J., dissenting)). Even so, the search here was properly circumscribed by the terms of the warrant that FBI agents could only seize information reasonably related to an illegal steroid crime for which probable cause existed. The agents could have not have seized any computer within the Millersville facility absent some indication it might contain the data they were searching for. They could not have "seized the Zip disks under the bed," so to speak. (Op. at 13 (citing *United States v. Hill*, 322 F.Supp.2d 1081 (C.D. Cal. 2004))). As StarTests personnel pointed out to agents who arrived in the scene, most of the computers in the facility included at least one database on the CFL drug test. (R. at 2.) In

addition, the CFL was one of StarTests's largest clients, providing it with large amounts of information over the span of a four-year period (R. at 2.) Most importantly, StarTests deliberately employed an information dispersal technique known as "computer-hopping," which made the information for which probable cause existed impossible to isolate without a full search of the seized computer data.¹ As the Ninth Circuit warned in *Meek*, "the prohibition of general searches is not to be confused with a demand for the precise ex ante knowledge of the location and content of evidence related to the suspected violation." 366 F.3d at 706. Here, the Fourteenth Circuit has made that exact mistake and should be reversed.

B. The Fourteenth Circuit Incorrectly Applied *Tamura* To A Single File Of Information

The Fourteenth Circuit erroneously held that the government here improperly seized units containing information authorized for seizure intermingled with information not described in the search warrant. In doing so, it skipped straight to a *Tamura* analysis for intermingled files without first assessing whether the files at issue in this case were indeed separate and intermingled. Although the facts set forth by the district court and the Fourteenth Circuit are somewhat unclear on this point, they suggest that all of the drug testing information maintained in StarTests's hard drive were part of a single large file, making *Tamura* analysis unnecessary.

In *United States v. Tamura*, 694 F.2d 591 (1982), the Ninth Circuit considered whether the government could seize a *set* of hard-copy files including target data as well as information not specified in the search warrant. Unable to locate the files specified in the warrant without the assistance of the employees there, government agents seized all of the company files, including

¹ Essentially, StarTests maintained three databases for each drug test: one for the tests results with assigned ID numbers given to each participant, one for the names and personal health information of all the players, and still another which revealed the assignment of ID numbers to individual team members. Each one was saved on a different computer and under a different name. No one computer at the StarTests facility had two databases from any one test administered in any one year. (R. at 8.)

separate files not specified in the search warrant. *Id.* at 595. The Ninth Circuit condemned such “wholesale seizure for later detailed examination of records not described in a warrant.” *Id.*

However, in the earlier case of *United States v. Beusch*, 596 F.2d 871, 876-77 (9th Cir. 1979), the same court dealt with a motion to suppress evidence consisting of hard-copy ledgers containing items covered by a search warrant intermingled with items not covered by the search warrant. Noting that the appellants in that case cited no authority for the proposition that pages in a single volume must be separated by searchers so that only those pages which actually contain the evidence sought may be seized, the court held that such a rule would “substantially increase the amount of time required to conduct a search” and would require the use of “auditors, bookkeepers and accountants” to suss out the relevant information. *Id.* at 876-77. Because burdening police with such tasks would be impractical, the Ninth Circuit concluded that as long as an item appears at the time of the search to contain evidence reasonably related to the purposes of the search, there is no reason absent some other Fourth Amendment violation to suppress it. *Id.* at 877. The fact that an item seized happens to contain other incriminating information not covered by the terms of the warrant does not compel its suppression, either in whole or in part. *Id.*

In order to avoid “making a mockery of *Tamura*,” the Fourteenth Circuit admonished the government here for seizing all the computer equipment and files suggested instead sorting the evidence with some “procedure or plan.” (R. at 14.) The opinion discusses that the relative ease with which the government could have parsed the relevant information for which probable cause existed: the agents could have simply located the database with the identification numbers, then located the database with the test results, matched the numbers to the results, and then performed a cut-and-paste function of the drug test results into another document. (R. at 14-15.) Setting

aside for a moment a discussion of whether such actions would have indeed been a “simple procedure” as the Fourteenth Circuit supposed, such actions were not required under *Tamura* and *Beusch*. In *Beusch*, government agents seized records and ledgers containing evidence of criminal activity. Because the ledgers were arranged in alphabetical order by client, it was possible for government agents to separate the evidence for which probable cause existed from the other records the ledger contained. *Id.* at 873. However, the Ninth Circuit concluded in *Beusch* that no Fourth Amendment violation occurred when agents seized “single files and single ledgers, i.e., single items which, though theoretically separable, in fact constitute one volume or file folder.” *Id.* at 877.

Although the facts in the record are slightly unclear on this point, they suggest that the evidence relating to the five players for which probable cause existed was mixed in with information on third parties *within a single file*. As the Fourteenth Circuit acknowledges, at the very least all records searched were contained within the same “test results” hard drive, which contained only the substance use results of each player in the league. (R. at 9.) Because the information used to expand the investigation to other players was found in the same file as those results, such as a single Excel Spreadsheet, and not in separate “closed files,” the Fourteenth Circuit’s application of *Tamura* to the facts of this case is misguided. *Cf. U.S. v. Carey*, 172 F.3d 1268, 1273 (10th Cir. 1999) (invalidating a search of all but the first .jpeg file opened by police, because the rest were “closed files” that could not have been expected to yield any information related to the search for which probable cause existed). The Fourteenth Circuit thus erred by concluding that the government violated the Fourth Amendment by seizing and searching separate, intermingled files for which there was no probable cause to search. As the Ninth Circuit noted in *Beusch*, the “Fourth Amendment confers a great many specific protections

against unreasonable searches and seizures, but it does not confer upon persons subject to a lawful search the right to decide for himself what will and will not be seized. 596 F.2d at 876-77.

C. The Special Warrant Procedures For Computer Searches Set Forth in Comprehensive Drug Testing Are Neither Required By Nor Advisable Under The Fourth Amendment

The Fourteenth Circuit was unwise to wholly adopt the heightened warrant requirements set forth by the Ninth Circuit in *Comprehensive Drug Testing*. As Judges O’Neida and Whitney lamented in the dissent below, the Fourteenth Circuit has decided to follow in the footsteps of a “renegade” Ninth Circuit case, disregarding clearly established precedent and detrimental to the investigatory abilities of law enforcement officials. (R. at 18).

A majority of courts do not require warrants to specify the government’s search methodology for computer searches. *See, e.g., U.S. v. Brooks*, 427 F.3d 1246, 1251 (10th Cir. 2005) (holding that warrants have never been required to contain a particularized search strategy, but only the objects of the search); *U.S. v. Adjani*, 452 F.3d 1140, 1150 (9th Cir. 2006) (refusing to limit search of emails to specific email addresses or search terms); *U.S. v. Gray*, 78 F.Supp.2d 524, 530 n.8 (E.D. Va. 1999) (holding that despite the possibility of using search programs to determine whether a file contained pictures or test without opening it, it would be unreasonable to force the government to always use the most advanced search techniques); *U.S. v. Vilar*, No. 05-CR-621, 2007 WL 1075041 (S.D.N.Y. Apr. 4, 2007) (describing the “majority view” is not to limit the governments search protocol). It is true that many scholars have argued that computers pose a unique Fourth Amendment problem, due in large part to the immense amounts of information they can store, and the fact that such information tends to span a range of different purposes. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531,

569 (2005) (noting, for example, even office computers are used as “postal services, playgrounds, jukeboxes, dating services, movie theaters . . . and more”). Despite these unique constitutional challenges, courts have held that the ultimate Fourth Amendment standard is the same for both computer and hard-copy searches: reasonableness. *See Hill*, 459 F.3d at 974 (“As always under the Fourth Amendment, the standard is reasonableness.”). Thus, there is neither a heightened protection nor a reduced level of protection for information stored on computers, as there is “no justification for favoring those who are capable of storing their records on computer over those who keep hard copies of their records. *Vilar*, 2007 WL 1075041, at *36. *Accord U.S. v. Gray*, 78 F.Supp.2d 524, 584 (E.D. Va. 1999).

Cutting against heightened protections for computer searches is the fact that evidence of criminality is easy to disguise and hard to discover. Among the courts that have consistently upheld the validity of warrants in computer searches, this has been cited this as a chief concern. *See Adjani*, 452 F.3d at 1150 (refusing to limit search of emails to specific addresses or search terms because the files could be easily disguised or renamed); *Hill*, 459 F.3d at 978 (“Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer.”). The regularly applied rule is that the government is not required to trust computer file labels because it is easy for even the casual computer user to create misleading file names, or even make one type of electronic data appear to be another. The affidavit provided by the police in *Comprehensive Drug Testing* detailed some of these techniques, including giving a file a misleading name (pesto.recipe in lieu of blackmail.photos), a false extension (.doc instead of .jpg), encrypting the data, or booby- trapping the computer to “destroy or alter data if certain procedures are scrupulously followed. 579 F.3d at 995. Only the Tenth Circuit has found it appropriate to halt

the war on these widespread deception techniques by acknowledging the validity of self-labeled files in certain contexts. *U.S. v. Carey*, 172 F.3d 1268 (10th Cir. 1999) (invalidating all but the search of the first .jpeg file opened during the search of a personal computer). However, subsequent decisions have made clear that *Carey* was “predicated only upon [its] particular facts.” *United States v. Giberson*, 527 F.3d 882, 890 (9th Cir. 2008). Specifically, the officer in *Carey* had testified that upon opening the remaining .jpg files, “he expected to find child pornography and not material related to drugs,” and that when he thereafter searched the .jpg files, he was looking for child pornography, and not drug-related material. 172 F.3d at 1273.

Another potential complication regarding computer searches is the fact that often, because of time restraints and insurmountable technical limitations, such searches cannot be carried out at the time the warrant is executed on the premises. *Vilars*, 2007 WL 1075041, at *35. *See also Hill*, 459 F.3d at 974-75 (observing that “there is a serious risk that the police might damage the storage medium or compromise the integrity of the evidence by attempting to access the data at the scene,” and that taking the time needed to search a computer at the scene “would not only impose a significant and unjustified burden on police resources, it would make the search more intrusive”). As a result, it is frequently the case with computers that the normal sequence of ‘search’ and then selective ‘seizure’ is turned on its head, as computer hardware is seized from a suspect’s premises before its content is known and then searched at a later time. *Vilars*, 2007 WL 1075041, at *35. *See also Hill*, 459 F.3d at 974 (holding that “the police were not required to bring with them equipment capable of reading computer storage media and an officer competent to read it). Instead of limiting searches to specific protocols detailed in a warrant, courts look to the object of the search, the types of files that may reasonably contain those objects, and whether officers actually expanded the scope of the search upon locating

evidence of a different crime. *Brooks*, 427 F.3d at 1252. In *Carey*, while searching for drug crime evidence, officers came across evidence of child pornography, and without authorization they expanded their search of a computer for additional pornographic images. 172 F.3d at 1269. In contrast to the search in *Carey*, government agents here did not extend the scope of the search to materials beyond those permitted by the warrant, and they had reason to believe the all the files seized contained evidence of the five named players' illegal steroid use.

In addition to forswearing reliance on the plain view doctrine, the Fourteenth Circuit has proposed essentially four additional safeguards against overseizure in electronic search cases based on the Ninth Circuit's opinion in *Comprehensive Drug Testing*. First, specialized personnel or an independent third party must perform the segregation and redaction of computer evidence. Second, warrants must disclose the actual risks of destruction or concealment of information. Third, the government's search protocol must be designed to uncover only the information for which it has probable cause, and finally, the government must destroy or return non-responsive data. (R. at 17.) The Fourteenth Circuit admits that the last of these prongs was satisfied because the Wythe warrant required the return of property irrelevant to the search. (R. at 15.) In addition, the warrant designated the tasks of seizure and data segregation to "appropriately trained personnel" in compliance with the first *Comprehensive Drug Testing* prong. (R. at 8.)

With regard to the demands imposed by the remaining requirements, this Court would be unwise to follow in the footsteps of the Ninth Circuit. Though the Fourteenth Circuit soothsays that this new standard will "force magistrate judges to more deeply scrutinize the warrant application" (R. at 13-14), in practice the more likely outcome will be to create confusion among magistrate judges issuing warrants in the digital era. As argued above, often law enforcement

officers do not know what data security programs they will come across in the execution of a search warrant, and so it would be impractical to require them to predict such risks in the warrant itself. Additionally, there is always a risk that any given computer could be rigged to destroy or alter the data if certain procedures are followed. These concerns are especially strong in the context of electronic data search of a company's computers that are equipped with programs to protect client confidentiality. Contrary to the Fourteenth Circuit's suggestion that specialized personnel could have isolated the relevant databases and performed a "cut and paste" function in order to ensure they would only view the information for which probable cause existed, no courts have ever required police to trust the labeling of databases or computer files. Constraining electronic searches in this way would make as much sense as instructing police in drug raids to ignore all white substances in bags clearly marked "flour." *United States v. Hill*, 322 F.Supp.2d 1081, 1090 (C.D. Ca. 2004).

Finally, to the extent that the third *Comprehensive Drug Testing* prong requires police to conduct an on-site inspection of electronic data to determine which files should be seized, strong precedent from various circuit courts cautions against this, due to the risk that data might be compromised by on-site access and the additional intrusion occasioned by the extended search. Therefore, instead of following in the footsteps of a renegade Ninth Circuit decision, this Court would be wise to pursue the path of least resistance and to follow the clear commands of a majority of other federal circuit courts, upholding the warrant at issue here.

D. The Comprehensive Drug Testing Warrant Procedures Are Incompatible With Recent Amendments To Rule 41(g)

Relying heavily on the detailed guidance from the Ninth Circuit presented in *Comprehensive Drug Testing*, the Fourteenth Circuit overlooked recent ESI-related amendments to Rule 41 governing search and seizure that have come into effect since that decision was

handed down. These amendments became effective December 1, 2009, just three months after *Comprehensive Drug Testing* was decided. They specifically contemplate the government's seizure, copying, and later review of ESI and storage media. A new Rule 41(e)(2)(B) provides: "unless otherwise specified, the warrant [for ESI] authorizes a later review of the media or information consistent with the warrant." As pointed out by the Advisory Committee, Subdivision (e)(2) "acknowledges the need for a two step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant." Fed. R. Crim. P. 41(e)(2)(B) advisory committee's note.

The Advisory Committee's notes indicate that the warrant requirements adopted in *Comprehensive Drug Testing* and by the Fourteenth Circuit below would be at odds with the Federal Rules on this point. To the extent that the Fourteenth Circuit's opinion can be read to require officers to conduct an on-site inspection and segregation of electronic materials in a database, that path is clearly foreclosed by the plain language of the amendment. In its opinion below, the Fourteenth Circuit held that to give effect to the requirement that "the government's search protocol must be designed to uncover only the information for which it has probable cause," the warrant must prescribe "any detection equipment or special equipment used to detect the databases and ascertain the information." (R. at 15.) This is at odds with the spirit of the amendment, which allows warrants to prescribe the wholesale seizure of computers and full copies of their contents without any limitations on sorting procedures or search protocols. Furthermore, the Fourteenth Circuit's requirement that segregation and redaction of computerized documents must either be done by specialized personnel or an independent third party is in tension with the Rule's acknowledgement that *officers* may seize or copy the storage medium *and review it later*. Fed. R. Crim. P. 41(e)(2)(B) (emphasis added).

The new Rule 41 also specifies that investigating officers “may retain a copy of the electronically stored information that was seized or copied.” Fed. R. Crim. P. 41(f)(1)(B). Application of the new rule would permit officers like the ones in this case to retain the copies of the computer hard drives seized at the StarTests Millersville facility, and, with proper judicial authorization, to draw from the copied drives information that could be used in a more extensive investigation into steroid use by the CFL players. However, a majority of the Fourteenth Circuit would have the police “destroy or return” the seized data, and seize it again from the Millersville facility each time probable cause arises with regard to substance abuse by another player. Although the Wythe warrant at issue in this case did indeed require the return of property irrelevant to the search, the permissive language of this amendment would have permitted a contrary result. This contrast illustrates that because magistrates may, and often do, find it appropriate to enact certain procedural safeguards in the warrant itself depending on the unique circumstances of each case, there is no reason to tie their hands by forcing them to follow the strict procedural rules set forth in *Comprehensive Drug Testing* and the opinion below.

Taken together, the new amendments to Rule 41 acknowledge the necessity of government “overseizure” in the ESI context, and carve out a broad area in which police may act pursuant to a facially valid warrant. These boundaries set by the amendments to Rule 41 serve not only as endpoints, but also as guideposts to proper police and magistrate conduct. The Fourteenth Circuit’s decision has rerouted this path, and if this Court is not careful to correct the judicial map, its officer-travelers who seek to obtain criminal information from electronic databases will in large numbers find themselves at a dead end.

III. THE FOURTEENTH CIRCUIT ERRED BY REFUSING TO EXTEND PLAIN VIEW DOCTRINE TO DIGITAL EVIDENCE SEARCHES

A. This Search Satisfies The Traditional Plain View Requirement

The Fourteenth Circuit erred by failing to apply the plain view warrant exception to the evidence of criminal activity discovered during the police search of the databases. It has long been recognized that in certain circumstances, a warrantless seizure by police of an item that comes within plain view during their lawful search of a private area may be reasonable under the Fourth Amendment. *Coolidge v. New Hampshire*, 403 U.S. 443, 465-471 (1971). Since *Coolidge*, this Court has been more specific with regard to the plain view requirements, stating that in order for evidence to be properly retained under this exception: 1) the officer must be lawfully present in the place where the evidence can be plainly viewed; 2) the officer must have a “lawful right of access” the object; and 3) the incriminating character of the object must be “immediately apparent.” *Horton v. California*, 496 U.S. 128, 136-37 (1990). In *Horton*, this Court disposed of the inadvertence requirement in plain view cases, holding that even though inadvertence is characteristic of most legitimate “plain view” seizures, it is not a necessary condition. *Id.* at 130. Rather, the Court found that “evenhanded law enforcement is best achieved by applying objective standards of conduct, rather than standards that depend upon the officer’s subjective state of mind.” *Id.* at 138. The Court reasoned that the particularity requirements of the warrant check abuse by police officers in searching for things outside the legitimate scope of the search. *Id.* at 139-140. In other words, magistrates have an incentive to list everything on the warrant that police can search for, because once all the listed items are discovered, the search must end. Though privacy concerns are often the justification for prohibitions on general searches and warrants, these concerns are misplaced “when the inquiry

concerns the scope of an exception that merely authorizes an officer with a lawful right of access to an item to seize it without a warrant.” *Id.* at 142.

Though *Horton* did not involve digital evidence, courts have applied the same principles of the plain view doctrine from that case to seizures involving digital evidence. Of the courts that have addressed this relatively recent phenomenon, most have held that the plain view doctrine applies to digital evidence searches. See *United States v. Carey*, 172 F.3d 1268, 1273-74 (10th Cir. 1999) (applying the plain view test but finding that the government failed the test when a detective deliberately abandoned his initial search to pursue a new line of evidence related to pornography); *United States v. Raney*, 342 F.3d 551, 554 (7th Cir. 2003) (holding that the plain view doctrine applied because the agent’s seizure of homemade adult pornography was related to defendant’s intent to abuse minors); *United States v. Wong* 334 F.3d 831, 838 (9th Cir. 2003) (using the plain view doctrine to admit evidence related to child pornography that was found during a search for evidence connected to a murder); *United States v. Adjani* 452 F.3d 1140, 1152 (9th Cir. 2006) (rejecting the argument that computers should be exempt from the plain view doctrine because “the fear that the agents may come across...personal information cannot alone serve as the basis for excluding evidence of criminal acts”); *United States v. Gray*, 78 F.Supp.2d 524, 528 (E.D. Va. 1999) (using the plain view doctrine to find that agents conducting a computer search were entitled to examine “all of the defendant’s files” to determine whether they fell within the scope of the warrant)

The way in which government agents seize additional information under plain view in electronic seizure cases is relevant to determine whether such searches will be upheld. In *Carey*, the police detective deliberately abandoned his initial search related to drug sales and distribution to pursue a new line of evidence relating to child pornography. *Carey*, 172 F.3d at 1273 (10th

Cir. 1999). This child pornography evidence was stored in closed files that, by their labels, the detective could tell contained pornography. *Id.* at 1273-74. Not only was child pornography outside the scope of the warrant, but also the fact that the detective ventured down a new research path on which he actually opened “closed” files that were obviously outside the scope of the warrant based on their file names, put the seizure beyond the plain view doctrine. *Id.* at 1273-74. By contrast, the Ninth Circuit in *United States v. Giberson*, 527 F.3d 882, 890 (9th Cir. 2008), determined that a “plain view” seizure of child pornography during the search of a hard drive for evidence of fraudulent identification was proper. The Ninth Circuit distinguished *Carey*, holding that the two cases were consistent because the officer in *Giberson* “continued his search for ID fraud instead of embarking onto a new research trail.” *Id.*

In this case, the three prongs of the plain view test were all met by the seizure of the additional test results. First, the FBI was lawfully present both in the physical lab where the records were seized and in the “cyberspace” where they viewed the additional records under the warrant issued by Judge Leon. *See supra*, part II.A. The FBI agents here additionally possessed a “lawful right of access” to the data because, unlike in *Carey*, the agents in this case discovered the information about the other players while on the search path authorized by the warrant. The third “plain view” requirement, that the criminal nature of the object be “immediately apparent,” is also met in this case. The test results of the other individuals, listed alongside the test results of the five investigated players, clearly displayed positive results for a myriad of illegal substances, such as cocaine, marijuana, and various hallucinogens. (R. at 2.) Given the nature of the administered drug test, it was immediately apparent to the government that a positive result alongside words such as “anabolic steroids” or “cocaine” indicated criminal activity (R. at 6.)

Furthermore, as the district court below correctly noted, the positive test results here have more of a persuasively open and incriminating character than the images in *Carey* and *Giberson*, because of the nature of data and how it was stored. (R. at 6.) The files in *Carey* were “closed,” and therefore could not be used as evidence of criminal activity. Likewise, the police in *Giberson* could only view the allegedly pornographic images through a thumbnail file. In the most extreme example, the government’s seizure of child pornography was upheld even though the images were unopened and were separate files from the evidence the police were looking for in the initial search. *Wong*, 334 F.3d 831 at 838. In this case, though, there were no closed files that needed to be opened, nor were the images only displayed on small thumbnails. The FBI agents only had to open the database, which they had legal access to via the warrant, in order to see the test results of the other players. (R. at 6.) Because of this, the data found in this search was even more “immediately apparent” as criminal than the information found in other cases where the plain view doctrine has been applied and the seizure upheld. Therefore, not only does the search in question meet the three-pronged requirement of the plain view doctrine set out in *Horton*, but it accords with the case law of most circuits that have addressed the plain view requirement as applied to digital evidence searches. In line with its own precedent and that of a majority of federal courts, this Court should uphold the seizure of the additional records under *Horton* and reverse the Fourteenth Circuit.

B. Heightened Fourth Amendment Protections Should Not Be Technology-Specific

Technology is always evolving, and thus a principle or rule based solely on technology-specific reasoning is “unwise and inconsistent with the Fourth Amendment.” *Giberson*, 572 F.3d at 887. Until its decision in *Comprehensive Drug Testing*, the Ninth Circuit had consistently rejected the creation of an alternate bright-line standard for digital evidence searches, keeping it

in line with the decisions of other circuit courts that have addressed the plain view doctrine in digital evidence cases. For example, in *Giberson*, the defendant argued for suppression on the grounds that computers are distinguishable from ordinary storage containers because of their ability to store “massive quantities of intangible, digitally stored information.” 572 F.3d at 887-88. The Ninth Circuit replied that “neither the quantity of information, nor the form in which it is stored, is legally relevant in the Fourth Amendment context.” *Id.* The creation of arbitrary “bright-line” exceptions to the plain view doctrine would actually create more problems that it would solve. *Id.* at 888. For example, such distinctions would force courts to become technology specialists, drawing lines and determining legal differences between a computer hard drive and an external hard drive, or between information stored in a day planner and information stored on a Blackberry. *Id.* The rule is not based on the type of technology, but rather focuses on a simple question: “whether or not it is reasonable to expect that the items enumerated in the warrant could be found therein.” *Id.*

Indeed, most courts have refused to distinguish digital searches from physical searches when applying the plain view doctrine. *See Wong*, 334 F.3d 831, 838 (applying the traditional plain view doctrine to child pornography found in defendant’s graphic files because the police were “lawfully searching for evidence of murder in the graphics files”); *United States v. Adjani*, 452 F.3d 1140, 1152 n.9 (9th Cir. 2006) (“[T]he fear that agents may come across...personal information cannot alone serve as the basis for excluding evidence of criminal acts.”). Though it is true that there is a greater potential for the “intermingling” of relevant and other material with computer documents, this alone is not enough to eschew the plain view doctrine in digital evidence cases. *Id.* Police officers most assuredly should exercise caution when searching computer documents; however, of all searches of documents where personal information could

be present and does not provide adequate justification for the creation of a different and heightened standard for searches involving computers. *Giberson*, 527 F.3d at 889.

Like the police search in *Giberson*, the agents in this case were merely searching a database that they already had lawful access to via the search warrant. Unlike the search in *Carey*, where the Tenth Circuit did not recognize the applicability of the plain view doctrine to digital evidence cases, the FBI agents in this case did not venture off their regular search path in order to find information about the other players. The agents discovered this new information while using a “clear search methodology” by “searching for relevant records in places where such records might logically be found.” *See v. United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001). Under the plain view doctrine, the evidence might have been illegally seized if the agents had opened new documents or had gone off on an unrelated search to find the test results for the additional players. In this case, however, the FBI merely opened the database, looking for the information specified in the warrant, and instantly saw, in plain view, the other test results indicating criminal activity. (R at 5.)

Under the Fourteenth Circuit’s heightened standard, however, the fact that the documents were stored electronically rather than in a file cabinet would mean that the agents could not use any of the seized materials. While it would be disingenuous to suggest that electronic storage databases are no different from ordinary file cabinets, the relevant question is rather whether the differences in the storage capacities of the two types of files justify the disparate legal treatment that the Fourteenth Circuit has suggested. A large majority of precedent on the issue suggests that they do not. The Fourth Amendment reasonableness requirement, as well as the plain view doctrine, still apply, just as they would in any other search. Therefore, this Court should

continue to resist adopting special standards for searches involving technology, and reverse the decision of the Fourteenth Circuit.

IV. THE GOVERNMENT'S CONDUCT WAS NOT SO EGREGIOUS AS TO REQUIRE A RETURN OF SEIZED PROPERTY UNDER RULE 41(G)

The Fourteenth Circuit's determination that the data in the StarTests Millersville facility was illegally seized and searched lead them to improperly conclude that such property required return under Fed. R. Crim. P. 41(g). Courts have long held that Rule 41(g) is an appropriate means of obtaining the return of property improperly seized by the government. *Comprehensive Drug Testing*, 579 F.3d at 1001. Though styled as a motion under a Federal Rule of Criminal Procedure, when the motion is made by a party against whom no criminal charges have been brought, such motion is in fact a petition that the district court invoke its civil equitable jurisdiction. *Id.* at 324. However, a return of property should only follow from a particularly egregious violation by the government. *Ramsden v. United States*, 2 F.3d 322, 324 (9th Cir. 1993). The Fifth Circuit noted in *Richey v. Smith*, 515 F.2d 1239, 1243-44 (5th Cir. 1975), that a "callous disregard for constitutional rights" was one of four factors to be considered in the court's equitable discretion to return property under Rule 41(g). To illustrate the difference between cases in which a "callous disregard" of constitutional rights occurred, the court compared cases where the seizure or property by government agents was pursuant to a search warrant subsequently challenged as invalid, with cases where government agents "have allegedly engaged in fraudulent or deceitful methods in order to gain access to a citizen's private papers." *Id.* at 1244 n.8. The latter types of cases are those in which return of property has been ordered. The facts here, however, are consistent with the former type of case, where police relied on a warrant later invalidated by a judicial aggrandizement of procedural protections in the specific setting of electronic searches. The FBI in this case would have had no way to know to conform

with such detailed requirements, and nothing in the record shows either the FBI or the Judge Leon acted in bad faith.

The Ninth Circuit in *Comprehensive Drug Testing* affirmed Judge Mahan's equitable discretion to return the property at issue, stating that when the government comes into possession of evidence by "circumventing or willfully disregarding limitations in a search warrant, it must not be allowed to benefit from its own wrongdoing by retaining the wrongfully obtained evidence or any fruits thereof." *Id.* at 1003. Applying similar logic, the Fourteenth Circuit's opinion below describes the record in this case as replete with enough information to conclude that the government displayed a "callous disregard" for StarTests' and CFL's constitutional rights. (R. at 16.) It cites two examples to support its conclusion: first, the government's seizure of the electronic information "essentially shut down the facility" at the Millersville StarTests location, and second, that once the government found the information for which it lacked probable cause, it "actively sought to keep the information and use that information to go after league players." (R. at 16.)

Addressing the first conclusion, the facts of this case indicate not that the government's actions caused the Millersville facility to shut down, but on the contrary, allowed StarTests to continue its daily operations with minimal interruption. As discussed in Pt. II.D, *supra*, Fed. R. Crim. P. 41(e)(2)(B) allows officers to *either* seize or copy the entire storage medium specified in the search warrant. Thus, it was within the discretion of the federal agents executing the warrant to seize "all computer records, files, and equipment," necessary to obtain information relating to the steroid use by the five players for which probable cause existed. It is undisputed in the facts that upon execution of the warrant, the FBI discovered the computer configuration at StarTests to be more complex than originally anticipated. (R. at 8). In fact, StarTests' procedure

of “computer-hopping,” discussed in Part II.B, *supra*, employed to protect client confidentiality from hackers or government seizures such as this one, rendered the job of isolating the discrete pieces of information for which probable cause existed near impossible. Despite that fact, the government refrained from seizing all StarTest computers as the warrant authorized, but instead seized only the portable databases, copying the hard drives of computers that were stationary or difficult to move. (R. at 8). Furthermore, there is nothing in the record to suggest that StarTests’ business operations were damaged by the actions of the FBI agents.

Secondly, the fact that the government plans to use the seized information in an ongoing investigation into steroid use by league players is irrelevant to a determination of whether the government showed a “callous disregard” for the rights of the CFL and StarTests when it seized the data pursuant to a search warrant. As the Ninth Circuit explained in *Adjani*, “there is no rule . . . that evidence turned up while officers are rightfully searching a location under a properly issued warrant must be excluded simply because the evidence found may support charges for a related crime (or against a suspect) not expressly contemplated in the warrant. 452 F.3d at 1151. Thus, because the StarTests search was lawful, the information seized in the search can be used to provide a legitimate basis for future warrants without a callous disregard on the part of the officers.

Finally, the respondents have not demonstrated that the retention of the property by the government is unreasonable under Rule 41(g). The Committee Note accompanying a 1989 Amendment to the Rule teaches that reasonableness under all of the circumstances must be the test when a person seeks to obtain the return of property. 124 F.R.D. at 428. *See also In re Search of Kitty’s East*, 905 F.2d 1367, 1375 (10th Cir. 1990); *United States v. Fitzen*, 80 F.3d 387, 388 (9th Cir. 1996). If the United States has a need for the property in an investigation or

prosecution, its retention of the property generally is reasonable. 124 F.R.D. at 428. Because here, the government's legitimate interests in expanding its investigation to other CFL players implicated in the seized records cannot be satisfied without those records, its continued retention of those records is not unreasonable. *See Fitzen*, 80 F.3d at 388. Because the government's seizures were not unreasonable, and because the derivative use of legally seized evidence is a commonplace lawful practice, the Fourteenth Circuit's conclusion that the government showed a "callous disregard" must fail, and this court must conclude that the Appeals Court abused its discretion by granting respondent's Rule 41(g) motion.

CONCLUSION

Based on the forgoing, the government Petitioner respectfully requests that the United States Supreme Court reverse the decision of the Court of Appeals.

Respectfully submitted,

Competition Number 1
Counsel for the Petitioners

January 13, 2010