

IN THE  
**Supreme Court of the United States**

---

UNITED STATES OF AMERICA,

*Appellant,*

v.

STARTESTS, INC., and the  
COLONIAL FOOTBALL LEAGUE,

*Respondents.*

---

On Writ of Certiorari to the  
Supreme Court of the United States

---

BRIEF FOR RESPONDENT

Team Number 22

*Attorneys for Respondent*

---

---

TABLE OF CONTENTS

	<u>Page</u>
Questions Presented.....	1
Opinions Below.....	2
Jurisdiction.....	2
Constitutional Provisions and Statutes Involved.....	2
Statement of the Case.....	2
Summary of the Argument.....	7
Argument	
I. The CFL has standing to bring a Rule 41(g) motion for the return of its illegally seized drug test results.....	9
A. The CFL is a “person” aggrieved by the FBI’s unlawful search and seizure of the drug testing results held by StarTests Inc.....	9
B. The CFL has a contractual obligation to protect the interests of its franchisees and players, and therefore qualifies for associational standing.....	13
II. The United States may not rely on the “plain view” doctrine to fulfill the Fourth Amendment’s warrant requirement in the digital search of the CFL’s drug test results.....	16
A. The evolution of the “plain view” doctrine and its relation to digital evidence.....	16
B. The FBI’s seizure and detainment of the CFL’s copied records and documents does not qualify for the “plain view” exception, therefore violating the Fourth Amendment Rights of the CFL.....	18
III. The court of appeals correctly applied the heightened particularity requirement to the Startests warrant authorizing the government to seize all computer equipment and files in the digital evidence context.....	22

A.	The peculiar nature of digital evidence mandates increased protection under the Fourth Amendment.....	22
B.	Obtaining a warrant for digital property.....	24
C.	Various approaches to digital property warrants.....	25
D.	A heightened particularity requirement protects basic privacy interests.....	29
E.	The mandates in <i>United States v. Comprehensive Drug Testing</i> ensure individual privacy and will not hinder government investigations.....	31
F.	The Fourteenth Circuit correctly applied the principles of <i>United States v. Comprehensive Drug Testing Inc.</i> , to find the Startests warrant invalid.....	32
	Conclusion.....	34

TABLE OF AUTHORITIES

<u>Cases</u>	<u>Page</u>
<i>Andresen v. Maryland</i> , 427 U.S. 463, (1976).....	24
<i>Arizona v. Hicks</i> , 480 U.S. 321 (1987).....	17
<i>Bell Atlantic v. Twombly</i> , 550 U.S. 544 (2007).....	10
<i>Coolidge v. New Hampshire</i> , 403 U.S. 443 (1971).....	19
<i>Davis v. Gracey</i> , 111 F.3d 1472 (10th Cir. 1997).....	26
<i>Horton v. California</i> , 496 U.S. 128 (1990).....	17, 18
<i>Hunt v. Washington</i> , 432 U.S. 333 (1977).....	14
<i>Marron v. United States</i> , 274 U.S. 192 (1927).....	24
<i>Matter of Search Warrant for K-Sports Imports, Inc.</i> , 163 F.R.D. 594 (C.D. Cal. 1995).....	28
<i>Payton v. New York</i> , 445 U.S. 573 (1980).....	16, 29
<i>Pennell v. City of San Jose</i> , 485 U.S. 1 (1988).....	5, 14
<i>Rakas v. Illinois</i> , 439 U.S. 128 (1978).....	
..... <i>passim</i>	
<i>Showengert v. Gen. Dynamics</i> , 823 F.2d 1328 (9th Cir. 1987).....	13
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979).....	13
<i>United States v. Barbuto</i> , 2001 WL 670930 (D. Utah 2001).....	23
<i>United States v. Campos</i> 221 F.3d 1143 (10 <sup>th</sup> 2000).....	30
<i>United States v. Carey</i> , 172 F.3d 1268 (10th Cir. 1999).....	23, 27, 30
<i>United States v. Clough</i> , 246 F. Supp. 2d 84 (D. Me. 2003).....	28

<i>United States v. Comprehensive Drug Testing, Inc.</i> , 473 F.3d 915 (9th Cir. 2006) (Thomas, J., dissenting).....	32
<i>United States v. Comprehensive Drug Testing, Inc.</i> , 579 F.3d 989 (9th Cir. 2009)..... <i>passim</i>	
<i>United States v. Dichiarante</i> , 445 F.2d 126 (7th Cir. 1971).....	20
<i>United States v. Gray</i> , 78 F. Supp. 2d 524 (7th cir. 2005).....	28, 29
<i>United States v. Hall</i> , 142 F.3d 988 (7th Cir. 1998).....	26
<i>United States v. Hill</i> , 322 F. Supp. 2d 1081, 1090 (C.D. Cal 2004).....	28
<i>United States v. Hunter</i> , 13 F. Supp. 2d 574 (D. Vt. 1998).....	28
<i>United States v. Hunter</i> , 13 F.Supp.2d 574 (D. Vt. 1998).....	23
<i>United States v. Layne</i> , 43 F.3d 127 (5th Cir.1995).....	27
<i>United States v. Stierhoff</i> , 477 F. Supp. 2d 423 (D. R.I. 2007).....	23
<i>United States v. Taketa</i> , 923 F.2d 665 (9th Cir. 1991).....	11, 13
<i>United States v. Torch</i> , 609 F.2d 1088 (4th Cir.1979).....	27
<i>United States v. Upham</i> , 168 F.3d 532 (1st Cir. 1999).....	25
<i>United States v. Walser</i> , 275 F.3d 981 (10th Cir 2001).....	22, 24
<i>United States v. Wong</i> , 334 F.3d 831 (9th Cir. 2003).....	29
<i>United States. v. Adjani</i> , 452 F.3d 1140 (9th Cir. 2006).....	19
<i>United States. v. Habershaw</i> , 2002 WL 33003434 (D.Mass.2002).....	25
<i>United States. v. Tamura</i> , 694 F.2d 591 (9th Cir. 1982).....	22, 23, 30
<i>Warth v. Seldin</i> , 422 U.S. 490 (1975).....	10, 15
<u>Constitutional Provisions</u>	
U.S. CONST. amend. IV.....	<i>passim</i>
U.S. CONST. art. III, § 2, cl. 1.....	14

Statutes and Regulations

28 U.S.C. § 1254(1) (2009).....2

Fed. R. Cr. P. 41(g).....10, 12

Fed. R. Cr. P. 41(h).....10, 12

Other Materials

MedicineNet, COCAINE, [https://www.medicinenet.com/cocaine\\_hydrochloride-topical/article.htm](https://www.medicinenet.com/cocaine_hydrochloride-topical/article.htm).....21

Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 532 (2005).....23

RayMing Chang, *Why the Plain View Doctrine Should not Apply to Digital Evidence*, 12 SUFFOLK J. TRIAL & APP. ADVOC. 31, 34 (2007).....16

U.S DEPT OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS pt. II.A (2002), <http://www.cybercrime.gov/s&smanual2002.htm>.....26

WebMd, STEROIDS, [http://www.webmd.com/search/search\\_results/default.aspx?query=steroids&sourceType=undefined](http://www.webmd.com/search/search_results/default.aspx?query=steroids&sourceType=undefined).....21



## QUESTIONS PRESENTED

1. Federal Rule of Criminal Procedure 41(g) allows a person aggrieved by an unlawful search and seizure of property to move for the property's return. An association has standing on behalf of its members when its members would otherwise have standing to sue in their own right. Whether the Colonial Football League (CFL) can sue on behalf of its player members for the return of illegally seized property?
2. Whether the court of appeals erred in holding that the petitioner's reliance on the plain view exception to the Fourth Amendment's warrant requirement was misplaced and thus constituted an illegal search and seizure of respondent's property in violation of their Fourth Amendment rights?
3. Whether the court of appeals erred in strengthening Fourth Amendment protection in digital evidence context by adopting the standards set forth in *United States v. Comprehensive Drug Testing, Inc.*, requiring the particularity requirement be heightened in the digital evidence context?

## OPINIONS BELOW

The opinion of the district court (Rep. App. 1-6) and the court of appeals (Rep. App. 7-19) are unpublished.

## JURISDICTION

The judgment of the United States Court of Appeals for the Fourteenth Circuit was entered. This Court's jurisdiction is invoked pursuant to 28 U.S.C. § 1254(1) (2009).

## CONSTITUTIONAL PROVISIONS AND STATUTES INVOLVED

The Fourth Amendment provides: "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 probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Relevant sections of the Federal Rules of Criminal Procedure provide:

41(g): A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.

\* \* \*

41(h): A defendant may move to suppress evidence in the court where the trial will occur, as Rule 12 provides.

## STATEMENT OF THE CASE

In response to the growing steroid and performance-enhancing drug controversy that plagued professional sports, the Colonial Football League ("CFL") required each of its franchises to submit its players for drug screening tests. (Rep. App. 1, 8). To facilitate the

required testing, the CFL hired StarTests, Inc. (“StarTests”) (Rep. App. 1, 8). StarTests is an independent business that specializes in administering drug testing and compliance programs for corporations, sports organizations, and other entities. As an incentive to enter the program, the CFL and StarTests represented to the various franchises and their players that the information gathered would remain confidential and anonymous. (Rep. App. 8) The only information that was to be released by StarTests was the percentage of players who had tested positive in order to determine the level of steroid usage in the CFL. (Rep. App. 8). If the level of usage was above five percent the CFL would perform additional testing throughout future seasons. The CFL has required drug testing every year since 2005. (Rep. App. 8).

In July 2008, the Federal Bureau of Investigation (FBI) began investigating five renowned professional football players from two famous American professional football organizations. (Rep. App. 7). The FBI believed that the players and possibly the organizations themselves were implicated as major distributors and users of illegal steroids. (Rep. App. 7). From the Wythe City Lightning, the FBI collected evidence regarding quarterback Barry Reynolds and wide receiver John Reeves. From the Marshall Phoenixes, the FBI collected evidence regarding three newly drafted rookies named Danny Rodriguez, Michael Fleming, and Ace Hall. (Rep. App. 7). Both the Lightning and Phoenixes are team franchises and members of the CFL. During the course of the investigation and from the evidence collected from the various franchises, the FBI presented a case for probable cause that each of the five players had tested positive for steroid use under the CFL testing regime. (Rep. App. 1, 8). As a result, it applied for a search warrant to seize material related to these findings from the Star Tests facility in Millersville, Wythe. The FBI, in a supporting affidavit, requested permission to seize urine samples, but most importantly it asked to seize “all computer records, files, and equipment”

related to the StarTests-administered tests. (Rep. App. 2). In support of this broad request, the FBI cited the difficulties common to all computer searches—the massive quantity of data at issue, the technical difficulty of locating, identifying, and retrieving files that can be hidden in various H or S drives, and the fact that viewing and possibly of decoding the data might have required software not available at the StarTests site. (Rep. App. 2).

Magistrate Judge Leon authorized the search warrant, but placed several and notable restrictions on the search. The warrant authorized 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 compute equipment itself.” (Rep. App. 2) Yet, three restrictions controlled the search. First, the search was to be limited to information “reasonably related to the investigation into the five named players’ illegal steroid use.” (Rep. App. 2, 8) Second, “law enforcement personnel trained in search and seizing computer data” were to determine whether a computer needed to be seized. (Rep. App. 2, 8). Third, if computers or other equipment were seized, “appropriately trained personnel” were to review the data, retaining the information authorized by the warrant and designating the remainder to be returned to StarTests. (Rep. App. 2, 8).

On November 1, 2008, the FBI executed the search warrant and quickly discovered that the computer system at StarTests was more complex than their initial investigation had revealed. (Rep. App. 2). StarTests utilized a computer hopping procedure to maintain client confidentiality. (Rep. App. 2). This system is complex and requires StarTests to maintain three separate large databases for each drug test: one for the test results with assigned identification numbers, one for the names and personal health information of all the players, and another which revealed the assignment of the identification numbers to individual team members. (Rep. App. 2). After this discovery, the computer forensics agent decided to seize all of the computer

equipment at StarTests that was capable of being moved. The hard drives from equipment that could not be readily confiscated were copied for further review at the FBI computer forensics laboratory in Wythe City. (Rep. App. 2, 8).

Over the next several weeks, the FBI searched the CFL databases for the test results of the five players in question. (Rep. App. 9.) Eventually the FBI found the test results for the players in question, however, during the search the FBI discovered positive results for numerous other players. The results pertaining to other players indicated the usage of illegal steroids, other narcotics, and marijuana. The FBI copied and retained all of this information and soon after announced that they were expanding the scope of their search to cover all illegal substance abuse by professional athletes. After copying all information to this new objective, the FBI returned the unneeded computer equipment and hard drives. (Rep. App. 2, 9).

### ***Proceedings Below***

In the United States District Court for the District of Wythe, StarTests and the CFL filed a motion under Fed. R. Crim. P. 41(g) requesting that the court return the seized property. In the timely filed motion StarTests and the CFL claimed that all of the evidence other than the information related to the five players was outside the scope of the warrant and therefore illegally seized. (Rep. App. 9). Justice Martin found that the CFL had standing to bring the suit and observed, under *Rakas v. Illinois*, 439 U.S. 128, 134-35 (1978), that “a person aggrieved by an unlawful search and seizure is either a victim [or] one against whom the search was directed.” (Rep. App. 3). The district court found that the CFL qualified as one against whom the search was directed. Using the language from *Pennell v. City of San Jose*, 485 U.S. 1, 7 n.3 (1988) the court held that the CFL was a qualifying association which “has standing to sue on behalf of its members when they would otherwise have independent standing to sue, the interests sought to be

protected are germane to the organization's purpose, and the claim asserted does not require the participation of the individual members of the lawsuit." (Rep. App. 3).

In regards to the legality of the StarTests search and seizure under the plain view doctrine, the district court applied the plain view exception to the warrant requirement. (Rep. App. 6). As such, the district court held that the FBI had a lawful right to access the computer and all the information contained therein. This access allowed the FBI to view the positive test results and the results from the individuals outside the scope of the investigation. Justice Martin concluded that that the results of other players were in plain view, and their retention by the FBI constituted a valid search. (Rep. App. 6). Finally, the court held that the warrant was facially valid since "it restricted the search to information related to the five players' drug testing information and placed the decision to move the computer equipment in the hands of trained personnel, rather than in the arbitrary judgment of a FBI agent." (Rep. App. 6) StarTests and the CFL appealed the decision of the district court.

The court of appeals reversed the district court's application of the plain view exception to the warrant requirement. (Rep. App. 17). In doing so the court adopted the Ninth Circuit's standards in *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009). (Rep. App. 17). Those standards set forth heightened warrant particularity requirements in the digital evidence context. The court found that the government seized the evidence pursuant to an overly broad warrant that failed to satisfy the adopted standards. Thus, the search was deemed an illegal search and seizure in violation of the Fourth Amendment.

The court fully adopted the reasoning of the district court's holding in regards to the standing issue. However, the court of appeals noted that CFL arguably has a "stronger ownership interest in the databases than StarTests does, and this interest would even outweigh its

vicarious representation of the players' privacy interests." (Rep. App 10). This was due, in part, to the fact that CFL paid to administer the tests and to store the confidential results in the computer databases. Justice Firehouse commented that this view was "supported by the fact that the government searched the StarTests facility to acquire the 'CFL drug test databases'" (Rep. App. 10). The court of appeals remanded with instructions for the district court to enter an order for the result of any and all digital equipment to the StarTests facility. The government appealed the court of appeals' ruling.

### SUMMARY OF THE ARGUMENT

- I. The CFL has standing to bring a Rule 41(g) motion before the court, because the CFL is a person aggrieved by the government's unlawful seizure of its databases, and because the CFL has an obligation to protect the interests of its franchises and players. The government incorrectly asserts that the CFL lacks standing based on outdated and misapplied law. Through a series of case law, and amendments to the Federal Rules of Criminal Procedure, courts and legislatures have established guidelines to determine proper standing requirements. Applying these guidelines to the present case it is clear that the CFL has a constitutionally guaranteed right to bring this motion for return of its property under Rule 41(g).
- II. The FBI's seizure of computers and hard drives from StarTests was illegal, and in violation of the CFL's Fourth Amendment rights. The petitioner admits that the search warrant did not authorize them to search for information regarding all CFL members. (Rep. App. 4). Nor does it contest the fact that it did not have probable cause to search for information relating to individuals other than the five players named in the search warrant. *Id.* However, the petitioner does incorrectly assert that the additional

information was legally seized under the “plain view” doctrine. *Id.* Constitutional mandate, case law, and public policy all contradict this argument. The petitioner may not rely on the “plain view” doctrine to fulfill the Fourth Amendment’s warrant requirement in the present case. Thus, the FBI’s seizure of the CFL’s documents and records was illegal.

III. Search warrants for digital property require a heightened particularity requirement in order to ensure the basic privacy interest of all Americans is upheld. Computers and their ability to store vast amounts of data and intermingled documents require such a heightened particularity requirement. Approaches which lower the particularity requirement are illogical and threaten to transform digital property warrants into general search warrants, which are prohibited by the Fourth Amendment. The best and most consistent approach to the heightened particularity requirement is outlined in *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th 2009). Under those standards, before issuing a warrant in a digital evidence case, a magistrate judge must observe the following guidelines: 1) Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases. 2) Segregation and redaction must be either done by specialized personnel or an independent third party. If the segregation is to be done by government computer personnel, it must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant. 3) Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora. 4) The government's search protocol must be designed to uncover only the information for which it has probable

cause, and only that information may be examined by the case agents. 5) The government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept. *Comprehensive Drug Testing Inc.*, 579 F.3d at 1006. Following these guidelines will not hinder the governments ability to investigate criminal matters; it will simply ensure that a basic privacy and constitutional right is protected.

In the instant matter the Fourteenth Circuit correctly applied the guidelines in *United States v. Comprehensive Drug Testing Inc.*, and found that the StarTests warrant was invalid. This Court should affirm the ruling of the Court of Appeals and adopted the heightened particularity guidelines.

#### ARGUMENT

#### **I. THE CFL HAS STANDING TO BRING A RULE 41(g) MOTION FOR THE RETURN OF ITS ILLEGALLY SEIZED DRUG TEST RESULTS**

##### **A. *The CFL is a “Person” Aggrieved by the FBI’s Unlawful Search and Seizure of the Drug Testing Results Held by StarTests Inc.***

The public’s right to privacy, free from unwarranted government intrusion, is a well-established American Tradition. U.S. CONST. amend. IV. The Fourth Amendment protects citizens from illegal search and seizures, and further requires that any legal search and seizures be reasonable. *Id.* For many years, the courts and legislatures have been refining this important field of law in an effort to balance due process and police effectiveness. Nowhere have courts and lawmakers spent more time deciding the application of this amendment than in the arena of seized property. Specifically, the Supreme Court has devoted much time to deciding under what circumstances individuals have proper standing to bring an action for the suppression or return of illegally seized property. Oftentimes this argument comes down to the complaining party’s

relationship to the seized property, and the personal nature of their Fourth Amendment claim. *See Rakas v. Illinois*, 439 U.S. 128, 134 (1978).

“A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property’s return.” Fed. R. Cr. P. 41(g). In 1989 Rule 41(g) was amended to include the language “or by the deprivation of property.” *Id.* In addition, the 1989 amendment separated motions to suppress and motions for the return of property. *U.S. v. Comprehensive Drug Testing*, 579 F.3d 989, 1001 (9th Cir. 2009). Prior to the amendments the two motions were codified in the same section. *Id.* The difference between a motion to suppress and a 41(g) motion bears considerable weight on the issue of standing in the present case. A motion to suppress, now contained in 41(h), ensures that law enforcement will not be able to use evidence illegally obtained at trial against a criminal defendant (exclusionary rule) Fed. R. Cr. P. 41(h). Rule 41(g) is much broader, in that it applies to the property and privacy interests of those affected by the seizure and calls upon the courts civil equitable jurisdiction to ensure those interests are protected. *Comprehensive Drug Testing*, 579 F.3d at 1001. Currently, the CFL finds itself experiencing the exact injustice Rule 41(g) was meant to alleviate. Under Rule 41(g), the CFL must plead sufficient facts demonstrating that it is aggrieved by the deprivation of the seized materials. *Bell Atlantic v. Twombly*, 550 U.S. 544 (2007). The CFL meets this burden because it owns the seized material, and used them in its ongoing course of business, this is no longer possible. Additionally, this Court has decreed that when performing this test the Court must accept all facts in the pleading as true. *Warth v. Seldin*, 422 U.S. 490, 501 (1975). Under this standard the CFL easily meets the standing requirements for a 41(g) motion.

The CFL is the owner of the seized electronic media and copied disks. In 2003, the CFL began to require that all of its franchises submit players for drug screenings. (Rep. App. 1). The

CFL encouraged cooperation by promising players that the results would be confidential and used for limited purposes. *Id.* It did so without prompting from any law enforcement or government agency. The CFL paid StarTest to conduct the tests in furtherance of its business interests. *Id.* StarTests analyzed the samples, and reported back to the CFL, and future CFL corporate policies depended on the results of these tests. *Id.* The agency relationship created by the principal (CFL) and its agent (StarTests) gave the CFL ownership rights in the work done pursuant to the two companies' agreement. StarTests was under a duty to protect the property interests the CFL had in the specimens taken and the results generated. Had StarTests refused to comply with the agreement, the CFL would have an action under applicable contract and/or agency law. The simple facts that the CFL paid for these services, enticed its franchises and players to participate, and was using the results to determine future business plans demonstrate that it is an owner of the seized materials. Further, StarTests maintained exclusive control over the specimens and the majority of documents was pursuant to a confidentiality agreement. This control is in no way indicative of the CFL's lack of ownership. Had anonymity not been such an important factor in the administration of these tests, the CFL itself may very well have retained the records, samples, and statistics. Secondly, the CFL is aggrieved by this seizure simply in that its property was seized illegally. The deprivation of this property is interfering with its current and ongoing business objectives, resulting in negative fiscal and synergistic consequences. The CFL is simply trying to preserve the integrity and economic well-being of itself and its members, which could easily be compromised if the government released the contents of the confidential documents. (Rep. App. 16).

The petitioner incorrectly argues that under *Rakas*, and *Taketa* the CFL does not have standing to bring a Rule 41(g) motion. *See U.S. v. Taketa*, 923 F.2d 665, 669 (9th Cir. 1999). It

purports that the CFL “was in no way a person aggrieved by an unlawful search and seizure.” *Id.* In *Rakas*, the court decided that only a “victim [or] one whom against the search was directed” has standing to bring the motion. *Rakas*, 439 U.S. at 134-35. The petitioner describes the CFL as an unqualified movant suing to challenge the search of a third party’s premises. (Rep. App. 10). However, this is simply not the case. Although, the physical premises of the CFL were never raided, and nothing was physically taken, the agreement between the CFL and StarTests creates sufficient ownership in the records seized by the FBI from StarTest property. Thus, when the government seized the documents in question; its search was *directed* at the CFL.

Even if the court finds that the CFL’s ownership interests are not sufficient to pass the *Rakas* test, the petitioner’s reasoning still lacks merit. *Rakas* stands for the proposition that third parties may not move to *suppress* evidence in which they have no sufficient interest. The present case does not involve the suppression of evidence; it involves the return of property. The petitioner’s confusion is understandable, as *Rakas* was decided before the 1989 amendments to Rule 41. *Rakas*, 439 U.S. at 128. The amendments clarified the distinction between motions to suppress under 41(h), and motions to return property under 41(g). As mentioned above 41(g) is significantly broader than 41(h) and can be utilized by anyone aggrieved by the deprivation of property. Fed. R. Cr. P. 41(g). A 41(h) motion to suppress can only be brought by criminal defendants. Fed. R. Cr. P. 41(h). Further, *Rakas* deals with a situation where the petitioners made no claim of ownership in the seized property. *Rakas*, 439 U.S. at 129. As described above, the CFL has a strong ownership interest in the property seized.

The petitioner goes on to note that the CFL had no reasonable expectation of privacy in the seized databases. (Rep. App. 10). Thus, the petitioner concludes that the CFL would not fall under the exception in *Taketa*. *Id.* This argument has little merit. In *Taketa*, the court found that

if a party has a reasonable expectation of privacy then he also meets the Fourth Amendment standing requirements. *Taketa*, 923 F.2d at 669. The court looks at this expectation of privacy from a subjective standpoint that must be objectively reasonable. *Smith v. Maryland*, 442 U.S. 735, 740 (1979). Seeing how confidentiality was the driving force behind the entire system set up between the CFL and StarTests, there is no doubt (subjectively or objectively) that the CFL had a reasonable expectation of privacy concerning the documents. If StarTests had released the results to the public, this would have been a clear breach of the agreement. Following this same logic, it is apparent that the CFL had not just a “reasonable expectation of privacy,” but an overwhelming necessity for privacy, so strong that had it not been guaranteed, the agreement would likely have never been made. Additionally, as the court made clear in a number of cases and reaffirmed in *Taketa*, ownership of the property is not controlling. *See U.S. v. Taketa*, 923 F.2d 665 (9th Cir. 1991), *Showengert v. Gen. Dynamics*, 823 F.2d 1328 (9th Cir. 1987). Therefore, the fact that the petitioner contests the CFL’s ownership of the documents is immaterial.

In addition to the reasons set forth above, the CFL has an obligation to protect the interests of its franchises and players. Therefore, under the doctrine of associational standing the CFL is qualified to bring a 41(g) motion for the return of the property

**B. *The CFL has a Contractual Obligation to Protect the Interests of its Franchises and Players, and therefore Qualifies for Associational Standing***

Aside from its own property interests in the seized documents, the CFL has a contractual obligation to represent its individual players and franchises. (Rep. App. 10). These interests certainly extend to the privacy and content of the players’ bodily fluids. *Id.* Thus, under the doctrine of associational standing the CFL can properly move for the return of the property pursuant to Rule 41(g).

In *Hunt v. Washington*, this court stated “An association may have standing to assert the claims of its members even where it has suffered no injury from the challenged activity.” 432 U.S. 333, 342 (1977). The same *Rakas* test used in cases of traditional Fourth Amendment standing, must be met to qualify for associational standing. The movant must still be a “victim or one against whom the search was directed, as distinguished from one whom claims prejudice only through the use of evidence gathered as a consequence of a seizure directed at someone else.” *Rakas*, 439 U.S. at 134-35. Associational standing serves as a caveat to the *Rakas* test. It allows associations to represent the interests of its members in a court of law. The availability of associational standing is predicated upon four elements laid out by the court in *Pennell v. City of San Jose*:

Associational or representational standing requires 1. Actual injury redressable by the court, 2. That association members would otherwise have standing to sue in their own right, 3. That the interests the association seeks to protect are germane to the associations purpose and 4. That neither the claim asserted nor the relief requested requires participation of individual members in the lawsuit.

485 U.S. 1, 6-8 (1988). When an association meets all four elements required by *Pennell* the reasons for its adoption becomes clear. Associational standing allows the judicial process to be carried out more efficiently for both courts and litigants. As both the District Court of Wythe and the Fourteenth Circuit wisely recognized the CFL meets all four of these requirements.

The first requirement of the *Pennell* test is founded in Article III of the Constitution. U.S. Const. art. III, § 2, cl. 1. It allows courts to hear only “cases and controversies.” *Id.* This is not at issue in the present trial, there is no argument espoused by the petitioner or the lower courts denying that the CFL is claiming a judicially redressable injury. The last three elements of the test are founded in the Fourth Amendment and have a direct bearing on the present case. The second element, whether association members have standing to sue in their own right, is also

met by the CFL. The franchises and more importantly the players who the CFL represents would all have standing under both Article III and the Fourth Amendment. (Rep. App. 3). The players gave the urine samples to the CFL for the purposes of furthering the interests of the association. They did so under an understanding of confidentiality, whereby neither the public, authorities, nor the CFL would know the results of individual player tests. (Rep. App. 1). These players went against their natural instincts of privacy and self-preservation to increase the integrity and success of the game they love. Once the conditions under which they agreed to do so had been broken, those individuals had every right to move for the return of their property before a court of law. The third prong of *Pennell*, whether the issue in the case is germane to the purpose of the organization, is also straightforward. The franchises and players became members of this league to be represented by the CFL. Never again will there be a set of circumstances more fitting for the CFL utilize associational standing and represent the interests of its members. As the District Court stated (and the Fourteenth Circuit Court affirmed), “the players’ privacy interests in the results are related to the CFL’s organizational purpose. (Rep. App. 3). Under their contracts, “[the] CFL is charged with protecting those interests.” *Id.* The District Court goes on to note that the CFL’s duty to protect the players’ privacy is especially important since the privacy intruded upon was due to a prerogative of the CFL. *Id.* Finally, the CFL fulfills the fourth element. The players do not need to be individual parties to the suit in order for court to effectively grant the required relief. In *Warth*, the court decided prospective relief can be granted to an association on behalf of its members, while monetary damages cannot. *Warth*, 422 U.S. at 515 (1975). In this case, the return of property awarded under the civil equitable jurisdiction of the court qualifies as the type of prospective relief contemplated in *Warth*.

Being that the CFL meets the four requirements of *Pennell*, it falls well within the definition of a “victim” under *Rakas*. Aside from meeting the necessary requirements for associational standing, the CFL qualifies for traditional Fourth Amendment standing because of the ownership interests it possesses in the seized documents. For the aforementioned reasons the CFL has standing to bring a Rule 41(g) motion for the return of its illegally seized property.

## II. **THE UNITED STATES MAY NOT RELY ON THE “PLAIN VIEW” DOCTRINE TO FULFILL THE FOURTH AMENDMENT’S WARRANT REQUIREMENT IN THE DIGITAL SEARCH OF THE CFL’S DRUG TEST RESULTS**

### A. *The Evolution of the “Plain View” Doctrine, and Its Relation to Digital Evidence*

Aside from guarding against unlawful search and seizures the Fourth Amendment requires that all warrants contain sufficient particularity and probable cause. U.S. Const. amend. IV. In effect, this clause serves to ban general warrants. As this court noted in *Payton*, “indiscriminate searches and seizures conducted under the authority of “general warrants” were the immediate evils that motivated the framing and adoption of the Fourth Amendment.” *Payton v. New York*, 445 U.S. 573, 584 (1980). This protection was originally drafted to protect one’s dwelling. However, with the great expansion of technology, the Fourth Amendment welcomes many personal things into its comfort and protection. However, in order to promote police effectiveness the courts have noted several exceptions to this protection over the years. One of the most formidable is the “plain view doctrine.”

The plain view doctrine is an exception to the Fourth Amendment. While it does not permit police to use general warrants to search private property, it does allow police to use evidence found that is technically outside the scope of a warrant. *See RayMing Chang, Why the Plain View Doctrine Should not Apply to Digital Evidence*, 12 SUFFOLK J. TRIAL & APP. ADVOC. 31, 34 (2007). A traditional example of the plain view doctrine is police pulling over a driver for

speeding, then upon speaking with the driver noticing a bag of marijuana on the front seat. While the original probable cause to pull the man over was for speeding, and not possession of marijuana, the officer may none the less use the marijuana as evidence at trial because it was in “plain view.” The requirement that the discovery of such evidence be inadvertent was eliminated by this court in *Horton v. California*, 496 U.S. 128 (1990). However, a large number of other cases have placed substantial limits on the doctrine. See *Arizona v. Hicks*, 480 U.S. 321 (1987) (finding that an officer violated defendant’s Fourth Amendment rights when he moved a stereo to record serial numbers with no probable cause). These restrictions become increasingly important in cases of the search and seizure of digital information. In this modern age computers store individual’s most private information, the exact kind of information the Fourth Amendment was designed to protect. Oftentimes, the sheer volume of digital information cause the problems faced by courts applying the “plain view” doctrine. It can be cumbersome to weed out information that the warrant allows the officers to search, from the information that it does not. In addition, unlike physical property in which there are spatial divides, computers offer no clear-cut boundaries. This causes many problems, and raises serious constitutional concerns. Often the original warrant paired with a liberal reading of the “plain view” doctrine, creates a general warrant, thus violating the Fourth Amendment.

Unfortunately, this is exactly the type of injustice the CFL is facing in the present case. The FBI armed with its original warrant paired with use of the “plain view” doctrine, turned what was a search for information relating to five players’ illegal use of one drug into a general warrant that reached not only to other players but also to different illegal activity. (Rep. App. 8-9). There are many interpretations of the “plain view” doctrine; in this case, the petitioner fails them all.

B. ***The FBI's Seizure and Detainment of the CFL's Copied Records and Documents Does Not Qualify for the "Plain View" Exception, therefore Violating the Fourth Amendment Rights of the CFL.***

In order for evidence to be lawfully seized under the "plain view" doctrine, the government must meet three requirements, promulgated by the Supreme Court in *Horton*: "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 to the object 3) The incriminating character of the object must be immediately apparent." *Horton.*, 496 U.S. at 136-137. Binding Supreme Court precedent and logical comparison of Circuit Court decisions, guide the application of this test. In the present case, the petitioner fails the *Horton* test. The agents were not lawfully present at StarTests facility, they did not have lawful access to the CFL databases, and the incriminating nature of the seized information was not immediately apparent.

The petitioner cannot prove the FBI met the first prong of the *Horton* test. As the District Court noted, a valid search warrant, or a person's consent can satisfy the lawful presence requirement. (Rep. App. 4). The FBI certainly did not have the consent of the CFL or StarTests to seize the disputed material. Furthermore, the FBI did not have a valid warrant to satisfy this first prong. The warrant issued by Judge Leon was overbroad and did not meet the particularity, or probable cause elements necessary to escape the Fourth Amendment's grasp. The insufficiency of the warrant is discussed in greater deal in section III. See *infra* (pp. 32-34).

The Petitioner is also unable to prove the second prong of *Horton*. The FBI did not have lawful access to the records and documents seized. This is true again because of the illegality of the warrant. See *infra* (pp.32-34). However, assuming *arguendo* that the warrant was proper, the FBI still did not legally access the information. This Court in *Coolidge*, stated that "the plain view doctrine may not be used to extend a general exploratory search from one object to another

until something incriminating emerges.” *Coolidge v. New Hampshire*, 403 U.S. 443, 466 (1971). In searches dealing with physical property deciding this prong is not difficult. However, when dealing with computers, gaining access to the computer is meaningless unless one has access to its files. *U.S. v. Adjani*, 452 F.3d 1140, 1152 (9th Cir. 2006). Oftentimes law enforcement will use a warrant for a computer search as an opportunity to review every file in the computer. They do so under the guise that they are looking for evidence related to the original warrant. The danger is then allowing the officers to invoke the “plain view” doctrine to use *anything* they find during the search as evidence for *any* crime. *See U.S. v. Hill*, 322 F. Supp 2d. 1081 (C.D. Cal. 2004). This treatment of the “plain view” doctrine is the type of exploratory search the court outlawed in *Coolidge*. To uphold its lawfulness would essentially nullify the affect of the Fourth Amendment. *Id.* Thus, there must be logical, constitutionally based limits to these digital searches.

In the present case, the agents could have complied with the limits of the warrant if they had shown a scintilla of restraint. The “computer hopping” system StarTests had in place offered a simple solution at the time, to what is now a complex issue. StarTests kept the CFL information in at least three separate databases. (Rep. App. 8). One database recorded the assignment of anonymous ID numbers to individual players, another gave the drug test result for each anonymous ID number, and a third gave personal health information about each player and contained nothing to do with the anonymous number. (Rep. App. 8 n.3). After the FBI executed the search warrant, a StarTest employee explained the process to them in detail. (Rep. App. 8). In order to comply with the warrant and the Fourth Amendment all the FBI had to do was go to the database with the list of names and corresponding anonymous numbers, note the numbers of the five players named in the warrant, find those numbers in the database with the drug test

results, and seize those results. The District Court argues that because there is no evidence of the FBI ending the search for the five players and beginning another unauthorized search for other players or types of drug use the search complies with *Coolidge*. (Rep. App. 5) (stating that agents may not perform a general exploratory search). This argument does not hold up to even light scrutiny. If the search was performed properly, the agents *would* have had legal access to the list of names and corresponding numbers. However, after that point they *would not* have had legal access to the database matching the numbers to the drug tests, save for the five players originally named in the warrant. When the agents took the time to match the names to the results, they began a general exploratory search. This search was in violation of the Fourth Amendment rights of the players, and the CFL.

The petitioner also fails to meet the third prong of the “plain view” doctrine. The incriminating nature of the evidence is not immediately apparent, for two reasons. First, nothing about the evidence was immediately apparent. There are no landmark cases dealing with this qualifying language, however, comparing a case from the Seventh Circuit with a Case from the Tenth offers logical guidelines. In *Dichiarante*, the Seventh Circuit found that the criminal nature of receipts was not immediately apparent because they had to be open and read. *U.S. v. Dichiarante*, 445 F.2d 126, 130-31 (7th Cir. 1971). In contrast, the Tenth Circuit allowed pictures of child pornography stored on a computer which an officer opened and read, purportedly on accident. *Carey*, 172 F.3d at 1273 n. 4. Based on the “computer hopping” system in place there is no plausible explanation for how the drug results could be immediately apparent using this or any reasonable criteria. The agents had to do far more than just open a document or book. The fact that there were multiple databases, with multiple players, over multiple years means that anyone trying to match the anonymous numbers to the player names

would have to take note of the numbers and move back and forth between databases. (Rep. App. 8 n.3). The agents essentially had to perform separate investigations, this violates the “plain view” doctrine stands. Secondly, the District Court argues that the presence of a positive test for cocaine, or steroids indicates immediate illegal activity. This is simply not true. Steroids have many legal, and medically valid uses. *See* WebMd, STEROIDS, [http:// www.webmd.com/search/search\\_results/default.aspx?query=steroids&sourceType=undefined](http://www.webmd.com/search/search_results/default.aspx?query=steroids&sourceType=undefined) (naming asthma, arthritis and joint pain as several legitimate steroid uses). Additionally, cocaine can often be used as a local anesthetic in eye, ear, nose, and throat surgeries. MedicineNet, COCAINE, [https://www.medicinenet.com/cocaine\\_hydrochloride-topical/article.htm](https://www.medicinenet.com/cocaine_hydrochloride-topical/article.htm). Although, the legitimate use of cocaine is admittedly rare, steroid use is quite common especially for the types of injuries experienced by football players. Thus, while players using steroids prescribed by doctors might violate the rules of the CFL, it in no way violates any Federal laws. To determine whether or not the player had a legitimate source of the drug, the agents would have had to look in the third database. Again, in light of the “computer hopping” process no person could reasonably argue that the illegality of the seized documents and records was immediately apparent.

This illegal seizure by the FBI is a perfect example of the type of privacy the Fourth Amendment was meant to protect. The FBI has unreasonably interfered with the privacy of the individual players, and the CFL. In place of the “plain view” doctrine a more enlightened view was recently purported by the Ninth Circuit, and adopted by the Fourteenth Circuit. In *U.S. v. Comprehensive Drug Testing*, 579 F3d. 989 (9th Cir. 2009) the court stated: if agents legitimately come upon incriminating “plain view” evidence during the search they should have it sealed and held, until a magistrate approves further search. It went on to say that seizable

evidence should be separated from the non-seizable by an independent third party. *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d , 1001-1004 (9th 2009); *U.S. v. Tamura*, 694 F.2d 591, 595-96 (9th Cir. 1982). This rule is best suited to serve the needs of law enforcement and at the same time uphold the Fourth Amendment. Both the Ninth and Fourteenth Circuits have eliminated the “plain view” doctrine as it pertains to digital information. (Rep. App. 13). Therefore, because the Fourteenth Circuit has adopted the preferable test for “plain view” evidence, and because the present case fails to meet each of the three elements in the traditional “plain view” test.

### III. **THE COURT OF APPEALS CORRECTLY APPLIED THE HEIGHTENED PARTICULARITY REQUIREMENT TO THE STARTESTS WARRANT AUTHORIZING THE GOVERNMENT TO SEIZE ALL COMPUTER EQUIPMENT AND FILES IN THE DIGITAL EVIDENCE CONTEXT**

#### A. ***The Peculiar Nature of Digital Evidence Mandates Increased Protection Under the Fourth Amendment***

The Fourth Amendment is intended to protect Americans by prohibiting unreasonable searches and seizures. U.S. CONST. amend. IV. The amendment’s protection naturally extends to digital property stored on computers and other electronic devices. But, of course, digital property is different from physical property. The Tenth Circuit, in *United States v. Walser*, correctly noted the difference:

The advent of the electronic age and the development of desktop computers that are able to hold the equivalent of a library’s worth of information, go beyond the established categories of constitutional doctrine. Analogies to other physical objects such as dressers or file cabinets, do not often inform the situations we now face as judges when applying search and seizure law. This does not, of course, mean that the Fourth Amendment does not apply to computers and cyberspace. Rather, we must acknowledge the key differences and proceed accordingly.

275 F.3d 981 (10th Cir. 2001). The warrant requirement and the accompanying plain view exception are precisely such an area of Fourth Amendment jurisprudence that requires us to acknowledge those key differences and tread carefully forward.

Digital storage devices can hold extremely large amounts of data. People now use computers and other electronic devices to hold and create any and everything. “Computers record and store a remarkable amount of information about what users write, see, hear, and do” *United States v. Stierhoff*, 477 F. Supp. 2d 423, 442 (D. R.I. 2007) (quoting Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 532 (2005)). Computers contain information relating to all aspects of an individual’s life, including business and personal documents, financial records, address and phone lists, and all sorts of communications. See Kerr, *supra*, at 532-40.

Computers can be analogized to vast warehouses which store hundreds of thousands of individual containers in the form of discrete files. Each container or file, in this warehouse potentially contains personal or business information entirely unrelated to that stored in other containers in other areas of the warehouse. See Kerr, *supra* at 533, 555. This configuration raises the predicament in which a search for incriminating information will often reveal a large amount of other unrelated and non-incriminating information. See *United States v. Tamura*, 694 F.2d 591, 595-96 (9th Cir. 1982). Various courts have acknowledged that computers contain such “intermingled documents” See *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999) (citing *Tamura*, 694 F.2d at 595-96); *United States v. Barbuto*, 2001 WL 670930 (D. Utah 2001) (“searches on computers are unique because of their abundant storage capacity and the likelihood of discovering ‘intermingled documents!...’”); *United States v. Hunter*, 13 F.Supp.2d 574, 583-84 (D. Vt. 1998) (“Computer searches present the same problem as document searches-

the intermingling of relevant and irrelevant material-but to a heightened degree.”); *Walser*, 275 F.3d at 986 (“Because computers can hold so much information touching on many different areas of a person’s life, there is a greater potential for ‘intermingling’ of documents and a consequent invasion of privacy when police execute a search for evidence on a computer.”) The very quantity and variety of information on a computer increases the chance that highly personal information, irrelevant to the subject of the investigation, will be seized in the search.

#### B. *Obtaining a Warrant for Digital Property*

The warrant provides the avenue in which the police enter into a lawful position where they may take advantage of the plain view doctrine. Therefore, it is vital to consider how a warrant for digital evidence is issued. The basic requirements for any warrant to be issued are: (1) neutral magistrate, (2) oath or affirmation (3) based upon probable cause, and (4) a description that particularly describes the object of the search. U.S. CONST. amend IV. The first three requirements are not at issue in this matter, and thus will not be addressed, however the particularity requirement is greatly affected by the peculiar nature of digital property.

Particularity is vastly important for warrants for digital evidence because particularity outlines the scope of a search. The purpose of the particularity requirement is to “prevent a general exploratory rummaging in a persons belongings.” *Marron v. United States*, 274 U.S. 192, 196 (1927). Particularity requires that the warrant must “particularly describe the place to be searched and the person or thing to be seized.” U.S. CONST. amend IV. In cases, concerning searches of digital evidence contained in computers other storage devices such as servers, many courts have found that broad language, allowing the search of all computer equipment in relation to a particular type of crime, satisfies the particularity requirement of the Fourth Amendment. The difficulty that magistrates and the courts have with digital evidence and the particularity

requirement concerns questions regarding the execution of digital evidence warrants and the privacy concerns implicated by the peculiar nature of digital property. Overall, it is important to remember “in executing a warrant responsible officials, including judicial officials, must take care to ensure that the searches are conducted in a manner that minimizes unwarranted intrusions on privacy.” *Andresen v. Maryland*, 427 U.S. 463, 480-81 (1976)

### C. *Various Approaches to Digital Property Warrants*

The First Circuit, in *United States v. Upham*, 168 F.3d 532 (1st Cir. 1999) held that a warrant outlining a search for “any and all computer software and hardware ... computer disks, disk drives ... any and all visual depictions, in any format or media, of minors engaging in sexually explicit conducted [as defined by the statute]” was valid because the seizure and off premises search of the computer and other equipment was “about the narrowest definable search and seizure reasonably likely to obtain the images.” *Id.* at 535. The court reasoned that the search of a computer, even for deleted information, was not “inherently more intrusive than the physical search of an entire house for a weapon or drugs.” *Id.* Notably, the First Circuit justifies the broad language in a warrant by highlighting the difficulty of searching a computer. *See also United States v. Habershaw*, 2002 WL 33003434, 7 (D.Mass.,2002) (A search warrant authorizing a search of computer and all disks, etc... was not overbroad because when searching for child pornography, a warrant authorizing the seizure and search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the images.).

The flaw in the logic of the First Circuit and the other courts which follow their logic is that search a computer is not inherently difficult. Modern computers contain powerful search programs built into their operating system. A computer forensic expert, and possibly even a well

trained teenager, could conduct a simple search of a computer to uncover incriminating information contained therein. Even the United States Department of Justice has recognized that computers can be effectively searched using a search strategy; reducing the difficulty of searching a computer. *See* U.S DEPT OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS pt. II.A (2002), <http://www.cybercrime.gov/s&smanual2002.htm>.

The Seventh Circuit in *United States v. Hall*, 142 F.3d 988 (7th Cir. 1998) held that a warrant authorizing a search of any “hardware, computer disks, disk drives, internal modems, tape drives, disk application programs, data disks, system disk operating systems” was sufficiently particular because the “items listed on the warrants were qualified by phrases that emphasized that the items sought were those related to child pornography.” *Id.* at 996-97. The reasoning of the Seventh Circuit was followed by the Tenth Circuit in *Davis v. Gracey*, 111 F.3d 1472 (10th Cir. 1997) in which the Tenth Circuit held that a warrant authorizing a search of “equipment pertaining to the distribution or display of pornographic material in violation of state obscenity laws” was sufficiently particular because it included only items that were relevant to criminal activity and not items that failed to related to pornography. *Id.* at 1479. The Tenth and Seventh Circuits have held that broad warrant language meets the particularity requirement finding that a connection to a crime is the key factor in determining whether a warrant is sufficiently particular to satisfy the Fourth Amendment’s demands.

However, in the above cases government agents did not uncover or use any new information during the lawful search. Thus, the privacy concerns and the intermingled nature of digital property were not directly implicated or addressed by the courts above. Further, under the logic of the Tenth and Seventh Circuit a warrants power could be greatly expanded so long as a

government agent could demonstrate some nexus to criminal activity. This is already accomplished by the probable cause requirement for warrants. Simply creating an overlap between the probable cause and particularity requirement removes the particularity requirement and violates both the letter and spirit of the Fourth Amendment's warrant requirement.

Other courts have focused on the state of mind of the agent who conducted the electronic search. In *United States v. Carey*, 172 F.3d 1268 (10<sup>th</sup> Cir. 1999) police discovered evidence of child pornography while searching the defendant's computer for drug related evidence. The officer admitted that he while he was opening other files he was looking for child pornography, and not for evidence relevant to the mandated drug investigation. *Id.* at 1274. On these facts, the court found that the officer's search was a general search, and thus prohibited by the Fourth Amendment. *Id.* at 1276.

Other courts have simply required lower particularity requirements for digital property warrants. Most courts argue that it is impossible to determine which files will be files will be relevant and the warrant may not be able to state specifically what should be searched and seized. *See United States v. Torch*, 609 F.2d 1088, 1090 (4th Cir.1979). Courts have acknowledged the need for the use of generic terms in warrants seeking evidence of child pornography and have upheld more general warrants if the warrant limits the discretion of the agents executing the search. *See Torch*, 609 F.2d at 1090 (holding sufficient a warrant for "records, documents and writings related to the transportation, sale and distribution in interstate commerce of lewd, lascivious and filthy films"); *United States v. Layne*, 43 F.3d 127, 132-33 (5th Cir.1995) (upholding two warrants describing materials to be sought and seized as follows: "assorted pornographic videotapes; assorted pornographic magazines; assorted devices;" and, in the second warrant, "Child pornography; records of victims; drawings; pictures; computer disks,

sexual devices; videotapes; child abuse books; magazines; audiotapes; and any other obscene or child pornographic material;” finding the warrants sufficiently limited officers' discretion in searching.).

Various District Courts have also had difficulty devising a workable standard in regards to digital property warrants and the particularity requirement. The court in *United States v. Clough*, 246 F. Supp. 2d 84 (D. Me. 2003) held a warrant was too general because it had “no restrictions on the search, no references to statutes, and no references to crimes or illegality.” *Id.* at 87-88. In *United States v. Hunter*, 13 F. Supp. 2d 574 (D. Vt. 1998) and *Matter of Search Warrant for K-Sports Imports, Inc.*, 163 F.R.D. 594 (C.D. Cal. 1995) the courts expressly disapproved of catch-all phrases which transformed a warrant into a general warrant because it authorized the search of all items on the premises without regard to the subject matter of the warrants.

Behind the various and fractured decisions regarding digital property warrants are the competing interest of the government and the accused. Notably the characteristics of digital evidence make it difficult for government investigators to locate the evidence specified on a search warrant in a timely fashion. Special problems arise in the areas of computer searches. For example, a criminal might encrypt the data, plant “booby traps” that would destroy the data if accessed incorrectly, and use misleading file names. *See United States v. Hill*, 322 F. Supp. 2d 1081, 1090 (C.D. Cal 2004) (“Computer images can be hidden in all manner of files, even word processing documents and spreadsheets. 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 their casual observer.”); *United States v. Gray*, 78 F. Supp. 2d 524, 529 (7th Cir. 2005) (“Hackers often intentionally mislabel files or attempt to bury incriminating files within

innocuously named directories.”). Because it is theoretically possible that any given target of an investigation will have instituted measures to hinder the search for evidence on his/her computer, there exist the potential that the computer search will be time consuming and invasive. The time consuming nature of these search often requires that the computers be removed off site and the possible evidence contained therein be searched by computer technicians at a later date. Since the government agents ultimately decide how much too actually take this creates a powerful incentive for them to seize more rather than less.

Juxtaposed to the government’s concerns, defendants have argued that there are heightened privacy concerns at stake in computer search cases because of the quantity and variety of data that computers can store, and therefore, courts should limit the scope of computer searches. Of particular concern is that some courts have applied the plain view doctrine with the low particularity requirement in manner that transforms searches executed pursuant to a warrant for digital property into general searches of the digital property. *See Gray*, 78 F. Supp. 2d at 529 (E.D. Va. 1999) (An FBI Agents discovery of child pornography during his search for evidence of computer hacking was admissible); *United States v. Wong*, 334 F.3d 831 (9th Cir. 2003) (Child pornography discovered during a search of defendant’s computer during a murder investigation was properly admitted under the plain view doctrine.) This, in effect, transforms digital property warrants into a species of de facto general warrants. The express language of the Fourth Amendment prohibits general warrants. *See U.S. CONST. amend IV; Payton v. New York*, 445 U.S. 573, 583 (1980) (“[I]t is family history that indiscriminate searches and seizures conducted under the authority of General Warrants were the immediate evils that motivated the framing and adoption of the Fourth Amendment.”)

D. *A Heightened Particularity Requirement Protects Basic Privacy Interests*

The peculiar nature of digital property, namely that computers contain vast amounts of intermingled data, mandates that a heightened particularity requirement be implemented for digital property warrants to protect an individual's basic privacy interest. A failure to implement a heightened particularity requirement would allow government agents to seize an enormous amount of personal property belonging to individuals not under any suspicion of criminal activity. Further, other approaches have proved unworkable, illogical, and threaten basic privacy interest. This was exactly the concern the court addressed in *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th 2009). In facts similar to the present case, the FBI raided various research facilities for evidence of illegal steroid use. At the facilities, the agents seized all the computer and other electronic storage equipment believed to contain information regarding steroid usage and test results. When the drug testing company moved to have the property returned the government argued that they had complied with the warrant's requirements and thus was not required to return the warrant because the evidence was in plain view once the examination of the computers had begun. *Id.* The court relied on *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982) to find for the drug testing company. In *Tamura*, the Ninth Circuit held that in instances where documents are so intermingled that they cannot be feasibly sorted on site, . . . the Government . . . generally can avoid violating fourth amendment rights by sealing and holding the documents pending approval by a magistrate of a further search." *Id.* at 595-96. The Tenth Circuit has also adopted the *Tamura* approach in the computer context. In *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999), the court held "where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the

conditions and limitations on a further search.” *Id.* at 1275. Further, in *United States v. Campos* 221 F.3d 1143 (10<sup>th</sup> 2000), the Tenth Circuit addressed the problem of intermingled documents noting:

“In searching computers that contain intermingled documents, i.e., documents containing both relevant and irrelevant information, law enforcement officers must sort the documents and then search only the ones specified in a warrant, and where the officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending a magistrate’s approval of the conditions and limitations on a further search of the documents; the magistrate should then require the officers to specify in a warrant which type of files are sought.”

211 F.3d at 1148.

The Ninth Circuit in *Comprehensive Drug Testing* following the theory of *Tamura* and *Campos* and noted the need for a heightened particularity requirement, noting that without such a requirement government agents will be enticed to seize “more rather than less . . . Why just that directory and not the entire hard drive? Why just his computer and not the one in the next room and the next room after that? Cant find the computer? Seize the Zip disks under the bed.” *Comprehensive Drug Testing*, 579 F.3d at 998. The Ninth Circuit continued “the point of the *Tamura* procedures is to maintain the privacy of materials that are intermingled with seizable materials, and to avoid turning a limited search for particular information into a general search.” *Id.*

E. ***The Mandates in United States v. Comprehensive Drug Testing Ensure Individual Privacy and Will Not Hinder Government Investigations.***

To maintain compliance with the Fourth Amendment and to prevent the government from utilizing general warrants the guidelines outlined in *Comprehensive Drug Testing* should be adopted. The Ninth Circuit stated “the government should, in future warrant applications,

forswear reliance on the plain view doctrine or any similar doctrine that would allow it to retain data to which it has gain access only because it was required to segregate seizable from non-seizable data.” *Id.* If the government fails to heed this warning, the magistrate judge must order that the seizable data be separated by an independent third party under the courts supervision. *Id.* The court further required that the government disclose the actual risks of concealment and destruction of evidence in any given computer search, and that the search must be designed to discover only the documents for which the government has probable cause to search for. *Id.*

Policies to the contrary would permit the government to seize all records in a file or computer because the documents were intermingled in the same place. This would put Americans’ most basic privacy interest in jeopardy. For example, without the guidelines the government could seize the medical records of anyone who had visited a doctor that kept patient records in a computer database or similar filing system, which also contained the date of a person whose information was subject to a search warrant. *See United States v. Comprehensive Drug Testing, Inc.*, 473 F.3d 915, 959 (9th Cir. 2006) (Thomas, J., dissenting). Any claims that the procedures outlined in *Comprehensive Drug Testing* will hinder the government’s ability to investigate crimes is misplaced. The procedure need not impose impossible burdens on law enforcement. After seizure, the data is secure and may be reviewed by a neutral and detached magistrate, rather than being secreted for review by governmental officials. The essential safeguard required is that the removal must be monitored by a magistrate.

F. ***The Fourteenth Circuit Correctly Applied the Principles of United States v. Comprehensive Drug Testing Inc. to Find the StarTests Warrant Invalid***

*Comprehensive Drug Testing* outlines four prongs to test the validity of a digital search warrant. First, the segregation and redaction of information obtained from computer documents “must be either done by specialized personnel or an independent third party.” *Comprehensive*

*Drug Testing, Inc.*, 579 F.3d at 1006. As the Fourteenth and Ninth Circuit noted “government agents obviously were counting on the search to bring constitutionally protected data into plain view of the investigating agents.” *Id.* at 999. If the segregation process reveals information outside the scope of the warrant the authorized personnel must not communicate said information without separate court approval. *Id.* at 1000-01. Presently, the FBI agents copied, retained, and used the information uncovered by the search to launch another investigation. (Rep. App. 9). No separate court approval was ever obtained when the agents uncovered information outside the scope of the warrant; which was limited to information on five players.

Second, “warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.”

*Comprehensive Drug Testing Inc.*, 579 F.3d at 1006. The FBI in the StarTests warrant completely failed to disclose any of the risks of destruction of the information, and the record is void of any reference to such disclosures. (Rep. App. 1-20).

Third, the search protocol must be designed to uncover “only the information for which it has probable cause, and only that information examined by the case agents.” *Comprehensive Drug Testing Inc.*, 579 F.3d at 1006. The StarTests warrant allowed the government agents to uncover related and unrelated information. Using the unrelated information the FBI sought to expand their investigation outside the scope of the original five athletes and illegal to steroids to include other athletes and all illegal substances. (Rep. App. 9). Further, the record is void of any search strategy employed by the FBI; giving them free reign over the computer databases. (Rep. App. 1-20). This essentially transformed the StarTests warrant into an unlawful general warrant.

Finally, “the government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed about when it has done so and

what it has kept.” *Comprehensive Drug Testing Inc.*, 579 F.3d at 1006. The StarTests warrant satisfied this requirement as it required the return of property irrelevant to the search. (Rep. App. 15).

Under the analysis mandated by *Comprehensive Drug Testing* it is clear that the warrant in this matter is overbroad and therefore invalid. This further renders the search of the StarTests facility invalid and all evidence seized was done so illegally.

#### CONCLUSION

The ruling of the Court of Appeals should be affirmed and the standards outlined in *United States v. Comprehensive Drug Testing, Inc.* should be adopted to ensure compliance with the Fourth Amendment and protect against illegal search and seizures.

*Respectfully Submitted,*

Team Number 22

*Counsel of Record*

January 12, 2010



Respondents Appendix  
(Rep. App.)