

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 RESPONDENT

TEAM 2

TABLE OF CONTENTS

| | |
|--|-----|
| TABLE OF AUTHORITIES | iii |
| CONSTITUTIONAL PROVISIONS..... | v |
| QUESTIONS PRESENTED..... | vii |
| STATEMENT OF THE CASE..... | 1 |
| OPINION BELOW | 4 |
| SUMMARY OF THE ARGUMENT..... | 6 |
| ARGUMENT | 9 |
| I. THE APPELLATE COURT CORRECTLY AFFIRMED CFL’S STANDING TO BRING A RULE 41(G) MOTION. | 9 |
| II. THE FOURTEENTH CIRCUIT CORRECTLY REJECTED THE APPLICATION OF PLAIN VIEW DOCTRINE TO THE FOURTH AMENDMENT’S WARRANT REQUIREMENT IN CASES INVOLVING DIGITAL EVIDENCE. | 10 |
| A. The U.S. Circuit Court of Appeals for the Fourteenth Circuit correctly chose to reject the application of the “plain view” doctrine to digital searches..... | 11 |
| B. Even if this court were to allow the government to rely on the plain view doctrine for digital evidence, it should narrow the scope of the exception and require police to obtain a new warrant before directing their investigation at evidence not included in the original warrant. | 15 |
| C. Policy considerations should also persuade the court to restrict the government’s ability to expand searches and prolong seizures without a new warrant..... | 20 |
| III. THE PARTICULARITY REQUIREMENT FOR WARRANTS MUST BE HEIGHTENED IN THE DIGITAL EVIDENCE CONTEXT, AND THE GUIDELINES ADVOCATED BY THE FOURTEENTH CIRCUIT BELOW AND IN <u>UNITED STATES V. COMPREHENSIVE DRUG TESTING, INC.</u> , 579 F.3D 989 (2009) SHOULD BE ADOPTED BY THIS COURT. | 22 |
| A. The particularity requirement should be heightened. | 22 |
| B. The guidelines advocated by the Fourteenth Circuit and the Ninth Circuit in <u>United States v. Comprehensive Drug Testing, Inc.</u> , 579 F.3d 989 (2009) should be adopted by this Court. | 24 |

CONCLUSION..... 31
PRAYER FOR RELIEF 32

TABLE OF AUTHORITIES

Cases

Arizona v. Hicks, 480 U.S. 321 (1987)..... 14, 15, 19
Coolidge v. New Hampshire, 403 U.S. 443 (1971)..... passim
Groh v. Ramirez, 540 U.S. 551 (2004)..... 22
Horton v. California, 496 U.S. 128 (1990)..... 12, 29
Johnson v. United States, 333 U.S. 10 (1948)..... 11, 27
Jones v. United States, 362 U.S. 257 (1960)..... 9
Katz v. United States, 389 U.S. 347 (1967)..... 11
Ker v. California, 374 U.S. 23 (1963)..... 28
Lopez v. United States, 373 U.S. 427 (1963)..... 26
Marron v. United States, 275 U.S. 192 (1927)..... 24, 27
Maryland v. Garrison, 460 U.S. 79 (1987)..... 26
Pennell v. City of San Jose, 485 U.S. 1 (1988) 9
Rakas v. Illinois, 439 U.S. 128 (1978)..... 4, 9, 10
Shelton v. Tucker, 364 U.S. 479 (1960) 24
Stanford v. Texas, 379 U.S. 476 (1965)..... 22
Terry v. Ohio, 392 U.S. 1 (1968)..... 21
Trupiano v. United States, 334 U.S. 699 (1948) 11, 27
United States v. Adjani, 452 F.3d 1140 (9th Cir. 2006) 13, 23
United States v. Alexander, 574 F.3d 484 (8th Cir. 2009)..... 17
United States v. Carey, 172 F.3d 1268 (10th Cir. 1999)..... 13, 16, 25
United States v. Dichiarinte, 445 F.2d 126 (7th Cir. 1971) 19

| | |
|--|--------|
| <u>United States v. Giberson</u> , 27 F.3d 882 (9th Cir. 2008) | 18 |
| <u>United States v. Hill</u> , 459 F.3d 966 (9th Cir. 2006)..... | 13, 29 |
| <u>United States v. Raney</u> , 342 F.3d 551 (7th Cir. 2003)..... | 17 |
| <u>United States v. Ross</u> , 456 U.S. 798 (1982)..... | 23 |
| <u>United States v. Tamura</u> , 694 F.2d 591 (9th Cir. 1982)..... | 19 |
| <u>United States v. Turner</u> , 169 F.3d 84 (1st Cir. 1999) | 15, 26 |
| <u>United States v. Ventresca</u> , 380 U.S. 102 (1965)..... | 22 |
| <u>United States v. Walser</u> , 275 F.3d 981 (10th Cir. 2001)..... | 13, 16 |
| <u>United States v. Wong</u> , 334 F.3d 831 (9th Cir. 2003) | 17 |
| <u>Warth v. Seldin</u> , 422 U.S. 490 (1975)..... | 10 |

Statutes

| | |
|-----------------------------|--------|
| FED. R. CRIM. P. 41(G)..... | passim |
|-----------------------------|--------|

Constitutional Provisions

| | |
|-----------------------------|-------|
| U.S. CONST. AMEND. IV | 4, 13 |
|-----------------------------|-------|

CONSTITUTIONAL PROVISIONS

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 probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

STATUTES INVOLVED

FED. R. CRIM. P. 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.

QUESTIONS PRESENTED

- I. Does the respondent, the Colonial Football League have standing to sue on behalf of its players for the return of illegally seized property under Federal Rule of Criminal Procedure 41(g)?
- II. May the government rely on the “plain view” exception to the Fourth Amendment’s warrant requirement in digital searches, i.e. searches of computers, hard drives, disks, etc.?
- III. May federal magistrates issue warrants authorizing the government to seize all computer equipment and files for later storing, 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, Inc., 579 F.3d 989 (9th Cir. 2009)?

STATEMENT OF THE CASE

In July, 2008, the Federal Bureau of Investigation (FBI) began investigating five professional football players for suspected illegal steroid use: Barry Reynolds and John Reeves, who play for the Wythe City Lightening, and Danny Rodriquez, Michael Fleming, and Ace Hall, who are with the Marshall Phoenixes.¹ (R. at 1.) Quarterback Reynolds and wide-receiver Reeves are well known MVP's, whereas Rodriquez, Fleming, and Hall are newly-drafted rookies. (R. at 7.) The FBI suspected the players of being involved in a steroid ring and had eyewitness evidence and taped conversations of the five players wanting to “keep the rivalry interesting,” advance statuses in the league, and work for increased salaries and endorsement deals by procuring steroids. (R. at 8.) To prove the players had actually used steroids and not just talked about using them, the FBI sought to review the drug testing records of these players. (Id.)

The Wythe City Lightening and the Marshall Phoenixes are both successful franchises within the Colonial Football League (CFL). In 2005, CFL sought to ensure compliance with federal and state drug laws, as well as its own integrity as an athletic organization, and instituted mandatory drug screening tests for all the players within its franchises.² (R. at 1.) CFL hired StarTests, an independent business specializing in administering drug tests for large organizations, to conduct the drug screening and to process the results. (Id.) The purpose of the mandatory screening was to ensure that no more than five percent of players within the CFL tested positive for illegal drug use, and StarTests assured the players that their results would remain confidential. In fact, CFL only saw the percentage of players that tested positive for

¹ The Fourteenth Circuit below records Barry's name as “John.” (R. at 7.)

² The District Court below states that CFL initiated drug screening in 2003. (R. at 1.)

illegal drug use and not the individualized results. CFL wanted to use this percentage to make a yearly determination about whether to increase its drug screening requirements. If more than five percent of its players tested positive for illegal drug use, CFL was committed to increasing its level of screening. (Id.)

The FBI, investigating the five players, applied for a warrant to search StarTests' Millersville, Wythe facilities. It requested in its affidavit permission to search "*all* computer records, files, and equipment" (emphasis added) related to StarTests-administered tests and listed several reasons for such a broad search. (R. at 2.) Magistrate Judge Leon allowed the broad search but placed two important restrictions on it: First, he said "appropriately trained" computer personnel should determine whether it was necessary to seize individual data sources and should conduct the search of any seized data. Second, Judge Leon insisted that the search and seizure be limited to information "reasonably related to the investigation into the five named players' illegal steroid use." (Id.)

When the FBI conducted its search of the Millersville StarTests facility on November 1, 2008, it discovered that StarTests kept the data related to CFL drug tests on several different computers. The company utilized a "computer-hopping" system of information storage in order to protect the privacy interests of its clients. (R. at 2.) StarTests assures the players who come in for testing that their results will remain completely confidential and will be used for statistical reporting purposes only. Their method of storing data helps ensure their promise. (R. at 1.) Such a system does not even allow individual StarTest employees to have access to both test results and player names, thereby protecting the players' anonymity and statistical purity. On one database, for example, StarTests records the players names and assigns them identification

numbers, and on another it stores the actual results of the drug screen by identification number. (R. at 2.)

The FBI opted to remove all StarTests' computer equipment for off-site search, or to copy what could not be conveniently transported. (Id.) Agents then searched the databases and matched identification numbers and results to individual players. In doing so, they discovered evidence of CFL players not named in the warrant who tested positive for steroid usage. (Id.) After discovering this information, the FBI expanded the scope of the investigation to include all illegal drug possession and sale within professional football. (Id.)

StarTests and the CFL filed a motion for return of the seized records that did not pertain to the five players named in the warrant under Rule 41(g) in the Federal Rules for Criminal Procedure.

OPINION BELOW

Respondents brought their Rule 41(g) motion in the District Court for the District of Wythe and argued the seizure of StarTests' records was illegal because it exceeded the scope of the warrant. (R. at 1.) The government argued that even though it did not have probable cause to retain the additional information, the evidence was lawfully seized under the plain view doctrine. (R. at 9.) The government also challenged the standing of CFL to bring suit under Rakas v. Illinois, 439 U.S. 128 (1978). (Id.)

Circuit Judge Martin denied Respondents' Rule 41(g) motion, finding that while CFL had standing to make the motion as a party aggrieved by a search or seizure, the plain view doctrine allows for the retention of additional information. The district court referenced a collection of sister circuit decisions that applied the plain view doctrine to electronic searches. (R. at 4.) Respondents then filed a timely appeal to the Fourteenth Circuit, claiming the district court erred in applying the plain view doctrine so broadly to digital evidence cases. The Government appealed the district court's finding that the CFL had standing to bring a Rule 41(g) motion and argued the district court's decision on the plain view doctrine should be affirmed. (R. at 9.)

Writing for the Fourteenth Circuit, Judge Freehouse affirmed CFL's standing to bring a Rule 41(g) motion. He reversed the district court's decision on the plain view doctrine, however, claiming the procedural safeguards of the plain view doctrine enumerated in Coolidge v. New Hampshire, 403 U.S. 443 (1971) do not afford the same protection to electronic data as they do to houses or automobiles. (R. at 12.) Since the application of the plain view doctrine to electronic data was an issue of first impression for the Fourteenth Circuit, the Court ordered the government to forswear the use of the plain view doctrine in its warrant application for electronic searches and adopt the standards for electronic searches dictated by the Ninth Circuit in United

States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009). (R. at 13.) The court ordered the return of all the property to the StarTests Millersville facility. (R. at 16.) Petitioner, the United States of America, now appeals both rulings.

SUMMARY OF THE ARGUMENT

The ultimate question at hand is whether the United States government illegally searched and seized evidence of drug tests from StarTests, Inc. and the Colonial Football League. Consequentially, the legality of the search and seizure will determine whether the evidence (the property) needs to be returned under a Federal Rule of Criminal Procedure 41(g) motion.

First, it is established that both StarTests and the Colonial Football League have standing to sue for the return of the seized property under Rule 41(g). In the case of StarTests, government agents conducted the search and seizure on StarTests' premises and confiscated computers and other various electronic equipment belonging to StarTests.

In the case of the Colonial Football League, it has standing to bring suit on the basis of being an association formed for the purpose of protecting the interests of its member franchises and individual players. Government agents illegally seized results of drug tests by individual players in the Colonial Football League. Because the individual players have a right to bring suit and because the Colonial Football League represents the players, the Colonial Football League has standing to bring suit so long as the individual players are not required to participate in the suit. Even if the Colonial Football League could not obtain standing as an association, it could claim standing on the basis of its ownership interest in the seized computers and associated data.

Second, the court should not apply the "plain view" exception to the Fourth Amendment's warrant requirement in the case of digital searches. Traditionally, the Fourth Amendment has protected people against "unreasonable searches and seizures" by requiring a warrant. The "plain view" exception has allowed for additional incriminating evidence, outside the scope of the search warrant, to be admitted if found in the course of the search. The traditional analysis undertaken for the "plain view" exception is inappropriate for digital evidence.

The traditional analysis had three requirements: (1) that the officer be lawfully present in the place where the evidence can be plainly viewed, (2) that the officer have a lawful right of access, and (3) that the incriminating nature of the object be immediately apparent. There are several problems when applying this analysis to digital evidence. First, lawful presence and lawful access are one and the same for digital evidence as one implies the other. Second, for digital evidence, it is often not possible to determine the contents without viewing the contents, thereby leading courts to give blanket permission for digital searches. This is akin to a general warrant, which has long been frowned upon by this court.

Even if the court allowed the government to rely on the plain view exception in digital searches, it should narrow the scope of the exception and require that police obtain a new warrant before targeting evidence not included in the previous warrant. In other words, if police seize evidence not targeted in the original warrant in the course of a lawful search, then the evidence can be included. However, police should not expand or change the target of the search without a new warrant. The only situation in which the police should be allowed to expand their search beyond the scope of the original warrant is if they face exigent circumstances. That is, the police need to have some urgent reason for the expansion of the search.

Also, as a matter of policy, the court should limit the government's ability to expand searches and prolong seizures without a new warrant. This needs to be done not only to protect constitutional rights but also because of the potential consequences brought about by searches and seizures not explicitly permitted by a warrant. In the present case, StarTests had its reputation compromised and the Colonial Football League had to deal with a breach of an agreement with its individual players.

Third, the particularity requirement for search warrants in cases involving digital evidence need to be heightened. As mentioned above, in the case of digital evidence, the traditional analysis required by the "plain view" exception fails, as it leads to blanket permission for search and seizure of digital evidence.

To address this problem, the court should adopt the guidelines advocated by the Fourteenth Circuit, as set forth by the Ninth Circuit. This is a necessity brought upon by changes in technology. By adopting the guidelines, the particularity requirement found in the Fourth Amendment will be preserved. Yet, the particularity requirement needs to be balanced against the needs of law enforcement in dealing with the complexities created by digital evidence. These guidelines will serve to guide a magistrate's decision in cases involving digital evidence.

The guidelines are as follows: (1) the traditional analysis involved in the "plain view" exception should not be applied in digital evidence cases, (2) segregation and redaction of computer evidence should be done by independent third parties, (3) warrants should disclose the risks of destruction and the risks of concealment, (4) the search protocol must be designed to uncover only that information for which there is probable cause, (5) the government must destroy, or if the recipient may lawfully possess it, return non-responsive data.

The reasoning for the first guidelines follows from the arguments against the "plain view" exception above. The second is necessary to discourage police from investigating potential evidence outside the domain of the original warrant. The third provides the magistrate with further information with the risks involved while the fourth serves to protect property interests in limiting what can be seized as well as privacy interests of the persons that information is about. The fifth guideline protects the property interests, something increasingly important as more and more personal data is digitized.

ARGUMENT

Because the issue on appeal is a question of law that involves the denial of a Federal Rule of Criminal Procedure 41(g) motion and therefore requires a determination of the reasonableness of search and seizure in a criminal matter, the court must review the appellate court's reversal de novo.

I. THE APPELLATE COURT CORRECTLY AFFIRMED CFL'S STANDING TO BRING A RULE 41(g) MOTION.

To initiate a lawsuit, a party is required to have standing. Generally, standing requires that the party assert its own legal rights and interests and that there be a case or controversy according to Article III of the Federal Constitution that can be resolved legally. To have standing in a case involving a search or a seizure, the party bringing the suit must be "legitimately on the premises." Jones v. United States, 362 U.S. 257, 267 (1960). In Rakas v. Illinois, 439 U.S. 128, 142 (1978), the court defined "legitimately on the premises" to mean that "a person can have a legally sufficient interest in a place other than his own home." Qualifying for standing also requires that the party be "aggrieved by an unlawful search and seizure" meaning that the party is a "victim [or] 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." Id. at 134. CFL has two possible bases for claiming standing, first as an association representing the interests of its member franchises and players, and second as the owner of the illegally confiscated drug testing data.

CFL is an association with a contractual obligation to protect the interests of its member franchises and players and it was against five of its players that the government directed its search. According to the three-prong test set forth in Pennell v. City of San Jose, 485 U.S. 1, 7

n.3 (1988), an association has standing to sue on behalf of its members only when the members have standing to file a lawsuit individually, the interests being protected by the association are related to the association's purpose, and neither the claim asserted nor the relief requested requires the participations of the individual members. In the case of CFL, the individual players not named in the lawsuit have standing because their testing information was allegedly seized unlawfully and the CFL must fulfill its organizational purpose by protecting the privacy of its players not participating in the suit. Thus, as an association, CFL seeks injunctive relief, not damages, so the individual players need not be involved in the lawsuit. Warth v. Seldin, 422 U.S. 490, 515 (1975).

Second, even if CFL cannot claim standing as an association, CFL can claim standing on the basis of its ownership interest in the seized databases and computer equipment. Although StarTests kept the information and the equipment, CFL paid for both the testing as well as the anonymous storage of records and thus owns the information. This satisfies the requirement that CFL be "legitimately on the premises." In addition, when the government raided the StarTests facilities, it directed its search towards the CFL drug testing information and thus against CFL. CFL therefore meets the requirements of standing under Rakas.

II. THE FOURTEENTH CIRCUIT CORRECTLY REJECTED THE APPLICATION OF PLAIN VIEW DOCTRINE TO THE FOURTH AMENDMENT'S WARRANT REQUIREMENT IN CASES INVOLVING DIGITAL EVIDENCE.

The Fourth Amendment protects people against "unreasonable searches and seizures." U.S. CONST. AMEND. IV. It also requires that warrants issued to allow the search and seizure of property are based on probable cause, and that these warrants describe with particularity "the place to be searched and the persons or things to be seized." A magistrate must assess probable cause before issuing a warrant. This is one of the protections of Fourth Amendment rights

because it requires “inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.”

Johnson v. United States, 333 U.S. 10, 14 (1948).

The digitization of property, however, in the last two decades has forcibly altered the way we must look at property and the ways in which it can be safeguarded from unreasonable searches and seizures. The traditional plain view analysis does not provide a reliable framework to guide magistrates and law enforcement when it comes to digital evidence, and the court should reject its application in those situations. Notwithstanding, if the court were to find the exception applicable, it should still hold that law enforcement may not expand a search or seizure beyond the scope of their warrant to include the evidence found in plain view without first obtaining a new warrant from a magistrate.

A. The U.S. Circuit Court of Appeals for the Fourteenth Circuit correctly chose to reject the application of the “plain view” doctrine to digital searches.

The court has always scrupulously reviewed the constitutionality of warrantless searches and seizures. It is a well-established principle that "searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment, subject only to a few specifically established and well-delineated exceptions." Katz v. United States, 389 U.S. 347, 357 (1967). Supreme Court jurisprudence has long shown wariness towards exceptions to the Fourth Amendment’s warrant requirement. The court has emphasized the need to prevent government from acting without a warrant when it searches or seizes evidence. Trupiano v. United States, 334 U.S. 699, 700 (1948).

One of the exceptions for a search warrant, the plain view doctrine, applies to situations, for example, “in which the police have a warrant to search a given area for specified objects,

and in the course of the search come across some other article of incriminating character.”

Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971). This exception generally makes great sense in the context of real property: if police officers are conducting a lawful search for evidence of one offense and come across evidence of another offense, the legality of their actions, as well as our concern for the public’s safety, requires them not to ignore the evidence before them but to act against this newly discovered crime.

The difficulty of the doctrine has been identifying “the circumstances in which plain view has legal significance rather than being simply the normal concomitant of any search, legal or illegal.” Id. As set forth by this court, the plain view test has three traditional prongs: (1) the officer must be lawfully in the place where the seized item was in plain view; (2) the officer must have "a lawful right of access to the object itself;" and (3) the item's incriminating nature must be "immediately apparent.” Horton v. California, 496 U.S. 128, 136-37 (1990). The court has also explicitly stated that “the 'plain view' doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges.” Id. at 136.

But the way that information is stored on a computer makes applying the plain view doctrine to digital evidence very difficult. This novel issue is a question of first instance before the court, as it was in the Fourteenth Circuit. The circuit court concluded that with digital evidence, “in nearly every case, the securing of a valid search warrant is sufficient to satisfy the first and second prongs.” (R. at 11.) However, the Court of Appeals wisely observed that such a distinction between the first and second prongs of the test “makes sense where there is an actual spatial difference between the place of entry and the object requiring effort to lift or seize.” (Id.) As the Fourteenth Circuit further noted about computers, “gaining access to the desktop is the same as having access to all the files in the My Computer folder.” (Id.)

Other circuits have also highlighted the difficulties posed by the search of a computer and the great risk to privacy this represents. Computers can be central stations for managing someone's life and include calendars and finances. Hence, computers have a great potential for intermixing documents and "a consequent invasion of privacy" when police execute a search. United States v. Walser, 275 F.3d 981 (10th Cir. 2001). Indiscriminate seizures could have a significant impact on someone's life. United States v. Hill, 459 F.3d 966, 977 (9th Cir. 2006). The Ninth Circuit noted that "[c]omputers are simultaneously file cabinets (with millions of files) and locked desk drawers; they can be repositories of innocent and deeply personal information, but also of evidence of crimes. The former must be protected, the latter discovered." United States v. Adjani, 452 F.3d 1140, 1152 (9th Cir. 2006). Computer files can all look identical or be labeled as the user wishes, which may easily lead a court to grant a blanket permission to search all of the contents of a hard drive. Suspects can hide computer files by disguising or renaming them, so some courts are understandably opposed to trusting a suspect's self-labeling. Id. at 1150. Or as the Ninth Circuit explained, "there is no way to know what is in a file without examining its contents, just as there is no sure way of separating talcum from cocaine except by testing it." United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006).

Some courts have taken this peculiar nature of computer files as circumstances allowing for broad (though in their view, just short of general) warrants. The Tenth Circuit, for example, implied that should files contained in a hard drive directory be ambiguous, a police officer would have permission to open every file in order to discover its contents United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999). But the line that divides such a search from a general warrant is rather thin. This court has already emphasized the "specific evil" of a general warrant, and of a "general exploratory rummaging in a person's belongings." Coolidge, 403 U.S. at 467. As the

Ninth Circuit cautioned in United States v. Comprehensive Drug Testing, Inc., “[I]f the government can’t be sure whether data may be concealed, compressed, erased or booby-trapped without carefully examining the contents of every file ... then everything the government choose to seize will, under this theory, come into plain view.” 579 F.3d 989, 998 (9th Cir. 2009).

General searches for digital evidence will likely result from trying to frame digital evidence in a traditional context where the plain view doctrine could apply. Computers are not like houses; they do not have typical divisions, such as walls, or separate storage spaces, such as drawers. Unlike in Arizona v. Hicks, 480 U.S. 321 (1987) police cannot go into a computer looking for one thing but keep themselves from investigating another because, as some courts have said, any file on a computer could be mislabeled. Even with database searches that allow police to search a hard drive like a search engine, police could claim that a suspect wrote his documents in code or removed key words to obstruct a search of the hard drive’s contents. The government would use this as an excuse to go through every file and searching and plain viewing would become the same thing. Therefore, any warrant that allows for a search of a computer will inevitably allow police to rummage through the entire contents of that computer, and every file will eventually be in plain view. In this case, that is exactly what happened. Magistrate Judge Leon’s restriction of the search to the five targeted players became meaningless because, once police gained access to StarTests’s computers, they could search every file by alleging that StarTests might have mislabeled files in order to protect the players, and thereby bring the entire contents of the computer into plain view. As case law shows, courts are willing to allow for broad searches of a computer’s content in that context and, in doing so, the prongs of the test meld together and wipe out particularity protections built into the warrant process. The plain view *exception*, therefore, becomes a broad, all encompassing pass to search anywhere on a

computer once police have obtained a warrant for a search; even if the warrant itself is narrowly tailored, the search will not be.

- B. Even if this court were to allow the government to rely on the plain view doctrine for digital evidence, it should narrow the scope of the exception and require police to obtain a new warrant before directing their investigation at evidence not included in the original warrant.

The FBI's conduct in this case did not meet the requirements of the first and second prongs because by expanding their search they exceeded the scope of Magistrate Judge Leon's warrant. The government should have limited its search to the five players whose names appeared in the warrant and should have obtained a new warrant before expanding its investigation to include illegal drug possession in general and the rest of the CFL.

In a well-known case of the pre-digital era, this court held that police cannot use a valid search to conduct a second search that is separate from the legal one. Arizona v. Hicks, 480 U.S. at 321. In Hicks police had gone into an apartment investigating a gunshot that appeared to have originated there. While in the apartment, they noticed what seemed to them to be stolen stereo equipment in plain view and proceeded to examine and move it. The court concluded that the distinction between "looking" at a suspicious object in plain view and "moving" it even a few inches is much more than trivial for the purpose of the Fourth Amendment when the police lack probable cause. Id. at 325. And because the stereo equipment was unrelated to the initial investigation and was unjustified by the exigencies of the situation, moving it constituted a new search and therefore a "new invasion of [respondent's] privacy." Id.

Decades later, the First Circuit expanded on the logic behind Hicks and began to apply it to a digital context in United States v. Turner, 169 F.3d 84 (1st Cir. 1999). In Turner a police officer conducting a consensual search of a house for evidence of an assault, came across a computer, in which he found evidence of child pornography. The circuit court suppressed the

evidence because the images did not fall within the “expressed object” of the intended search for evidence of an assault. Id. at 88. The broader message we can infer from this is if police specifically request permission to search for one kind of evidence, they can search for that evidence and seize other evidence they find during the lawful search. However, police may not expand the original search or change its stated target.

1. Even if they find evidence of criminal activity in plain view, government agents should not go beyond the scope of their warrant without further approval from a magistrate.

Appellate courts, such as the Tenth Circuit have applied this reasoning to digital evidence and upheld a clear preference for police procedure that calls for securing a new warrant before police can begin a new search that is separate from the original warrant. In United States v. Carey, 172 F.3d 1268 (10th Cir. 1999) officers performed a search for drugs and, in the process, seized two computers they found in plain view that they believed possessed evidence of drug dealing. Despite the specificity of the warrant, police opened files not pertaining to the sale or distribution of controlled substances and found child pornography. Id. at 1272. The circuit court held that the scope of the search went beyond that authorized by the warrant.

In United States v. Walser, 275 F.3d 981 (10th Cir. 2001), the Tenth Circuit upheld a search that began with a lawful plain view seizure because the officer did not start an investigation into the new evidence. In Walser, an agent lawfully searching a computer for evidence of drugs instead found child pornography. Id. When he did, in contrast to the agent in Carey, he ceased his search immediately and submitted an affidavit for a “a new search warrant specifically authorizing a search for evidence of possession of child pornography.” Id. at 985. The court found no fault in the fact that the officer opened a nondescript and unidentifiable file labeled “bstfit.avi” and inadvertently discovered the first image of child pornography on the

computer. Id. at 987. However, the court also cautioned that if the officer had conducted a more extensive search by “rummaging in folders and files beyond those he searched,” he might have conducted the equivalent of a wholesale search and exceeded constitutionally permissible grounds. Id.

The Eighth Circuit followed the Tenth Circuit’s precedent and upheld police search procedure because police sought a second warrant. United States v. Alexander, 574 F.3d 484 (8th Cir. 2009). There police reviewed evidence for invasion-of-privacy violations, but when the detective found child pornography instead, he stopped his review and asked for a second search warrant. Id. at 487. Other cases where courts have examined the extent to which an agent can expand his plain view search have upheld police actions if the expanded search did not relate the amount of permission police had. The Seventh Circuit upheld a police search and seizure because a suspect had given broad consent for police to search for child pornography evidence and police found adult pornography that they related “to the issue of [defendant’s] intent to abuse and exploit a minor sexually.” United States v. Raney, 342 F.3d 551, 558 (7th Cir. 2003). However, in the case of StarTests, investigating steroid sales by five players is a far less relatable search than investigating an entire league for the use of non performance enhancing (illegal) narcotics.

The Ninth Circuit has similarly upheld searches where officers restrained themselves and sought additional warrants. In United States v. Wong, 334 F.3d 831 (9th Cir. 2003), the court upheld the seizure of pornographic files uncovered during the search of a computer for murder evidence. In Wong, the investigating sergeant found the images during his lawful search for murder evidence, seized the computer equipment, and then applied for a new search warrant and submitted a statement of probable cause. Wong, 334 F.3d at 834. In both warrants, the

government also communicated what they sought with as much specificity as possible. Id. at 839. This circuit court reemphasized its view with its holding in United States v. Giberson, 27 F.3d 882 (9th Cir. 2008). In Giberson agents searched a computer for evidence of fraudulent identification (I.D.) materials pursuant to a valid warrant. During their search, one of the agents came across images of child pornography. Id. at 996. He printed out a sampling and continued to search specifically for I.D. materials. He obtained a new warrant to search the hard drive for images of child pornography and only then carried out a search for such material. Id. The court upheld the warrant and the search noting that it was “based on probable cause and clearly limited the types of documents and records that were seizable” and that it adequately restricted the discretion of the agents involved in the search. Id.

Through these holdings, circuit courts have demonstrated not only a clear preference for new warrants when searches are going to expand from what the original warrant specifies but also a concern for sufficiently limiting the discretion the government has in conducting its searches. In this case, the government might have conducted its initial search of StarTest computer records within the parameters of the warrant issued by Magistrate Judge Leon. However, as soon as it found some information on players and substances not covered by the warrant, the government did not go back to the magistrate for permission to expand the search. The government did not continue to look only for that which the warrant explicitly allowed. Instead it expanded the search and did not separate the computer data for return as the warrant specified. (R. at 2.) The government seized *all* of StarTests data and began to investigate *all* of CFL’s players for illegal narcotics *without probable cause*. The government could have continued to search for steroids in the records of the five players, seized any evidence found in *that* specific search, and sought a new warrant for the rest, but it could not, of its own accord,

change the object and scope of its investigation. Such actions are precisely what so many circuit courts wanted to prevent by upholding new and expanded searches only if the officers sought a new warrant to further investigate that which they had found in plain view.

2. Police should only be allowed to expand their search beyond the scope of a warrant if they face exigent circumstances.

Moreover, the police's seizure of the additional drug test results for players not specified in the warrant also demonstrates the unconstitutionality of the government's conduct. As the Seventh Circuit stated, the "expectation that an item may prove incriminating to a defendant in some unknown way, even if subsequent examination discloses the item is evidence of a previously unsuspected criminal activity, is not sufficient justification for the item's seizure." United States v. Dichiarinte, 445 F.2d 126, 129 (7th Cir. 1971). Another circuit court followed the same reasoning in saying, "It is highly doubtful whether the wholesale seizure by the Government of documents not mentioned in the warrant comported with the requirements of the Fourth Amendment. As a general rule, in searches made pursuant to warrants only the specifically enumerated items may be seized." United States v. Tamura, 694 F.2d 591, 595 (9th Cir. 1982). Furthermore, it underscored the seizure of documents not specified in a warrant as the type of action the Fourth Amendment intended to prevent. Id. The Tamura court also addressed the problem of intermingled documents by suggesting "that the Government and law enforcement officials generally can avoid violating Fourth Amendment rights by sealing and holding the documents pending approval by a magistrate of a further search...." Id. at 596.

While Arizona v. Hicks did hold that police in that case exceeded the boundaries of the plain view exception, the court in Hicks certainly did not want to see the exception eliminated if police confronted exigent circumstances. Arizona v. Hicks, 480 U.S. at 327 ("And the practical

justification for that extension is the desirability of sparing police ... the inconvenience and the risk, to themselves or to preservation of the evidence, of going to obtain a warrant.”). The court had previously alluded to such an exigency in Coolidge when it referenced situations where it was impractical to seek a warrant because the evidence could soon be moved or destroyed.

Coolidge v. New Hampshire, 403 U.S. at 460. But the court also contrasted these situations that imply a risk to evidence with those where police know the location of the evidence and the warrant requirement presents no real inconvenience. See e.g. Coolidge v. New Hampshire, 403 U.S. at 469.

At the time the government expanded its investigation to players not mentioned in the warrant for drug offenses not contemplated by the warrant, it faced no exigency of any kind that would have prevented it from sitting on the evidence until it could obtain a new or amended warrant to further investigate what it initially found in plain view. (R. at 2.) The FBI had already seized all of StarTests’ files and equipment and copied them, so they had no reason to fear the destruction of any of the evidence. In these situations we have seen other circuits uphold police searches when officers have sought new warrants, based on affidavits explaining the newly discovered probable cause for the search, and specifying the parameters of the new search and/or seizure. That the FBI found evidence of other illegal substances during their search for steroids did not give them permission to change the focus of their investigation to drugs not mentioned in the original warrant, which restricted search and seizure to information “reasonably related to the investigation into the five named players’ illegal steroid use.” (R. at 2.)

C. Policy considerations should also persuade the court to restrict the government’s ability to expand searches and prolong seizures without a new warrant.

The Fourteenth Circuit concluded that the government displayed a “callous disregard” for the constitutional rights of StarTests and the CFL. (R. at 16.) But more importantly, the circuit

court also took notice of the crippling effect the government's actions had on StarTests Id. StarTests has seen its reputation compromised and CFL has to contend with the breach of confidentiality to its players that the seizure represents. Id. Finally, both organizations must deal with the loss of their computer equipment and test records, which could result in the removal of football players from the field or with the complete paralysis of StarTests operations. Id. The circuit court additionally held that damages could scarcely compensate for the loss of business and reputation, and the "government's ability to continue to view the databases would forever breach the confidentiality agreement made with CFL's players." Id. Although that court ordered the return of all materials that police uncovered and seized outside the scope of the original warrant, StarTests and the CFL have already suffered great damage from the unlawful search and seizure.

Unlike the parade of *possible* horrors courts are warned about, what has occurred so far represents a parade of *actual* horrors. This parade underscores the need for the court to implement as many constitutional safeguards as possible to protect the citizenry from potentially crippling police action. If government agents are allowed to act as bloodhounds, and may pursue *any* scent their noses come across during the hunt regardless of whether it is their assigned prey, then "plain view" will no longer be an exception but rather a gateway to warrantless searches. Any agent that comes across incriminating evidence of the sort not covered by the warrant he is operating under at the time may feel free to initiate a new investigation into a new crime without ever having to show to a magistrate that he had probable cause for it. This will do away with most of the Fourth Amendment protections this court has enacted since Terry v. Ohio, 392 U.S. 1 (1968). As circuits who have already considered the issue of plain view exceptions in a digital context have shown, a magistrate's approval before beginning a new investigation is a necessity

before police can abandon the object of their original search in pursuit of a greater or broader goal. Unless police face an exigency such as the destruction of evidence, they should not be allowed to circumvent the warrant requirement

III. THE PARTICULARITY REQUIREMENT FOR WARRANTS MUST BE HEIGHTENED IN THE DIGITAL EVIDENCE CONTEXT, AND THE GUIDELINES ADVOCATED BY THE FOURTEENTH CIRCUIT BELOW AND IN UNITED STATES V. COMPREHENSIVE DRUG TESTING, INC., 579 F.3D 989 (2009) SHOULD BE ADOPTED BY THIS COURT.

A. The particularity requirement should be heightened.

Under the status quo application of the plain view doctrine, the particularity requirement of the Fourth Amendment becomes obsolete when applied to digital evidence. The Fourth Amendment states that warrants should issue “upon probable cause, supported by Oath or affirmation, and *particularly describing the place to be searched, and the persons or things to be seized*” (emphasis added). U.S. CONST. AMEND. IV. The particularity requirement is what distinguishes a properly-issued search warrant from a traditionally-abhorred general warrant, and the Supreme Court has stated that any warrant that fails to comply with the particularity requirement of the Fourth Amendment is unconstitutional. Stanford v. Texas, 379 U.S. 476, 559 (1965). Great deference is given to magistrates to determine probable cause and particularity. United States v. Ventresca, 380 U.S. 102, 109 (1965). In the digital evidence context, however, practical law enforcement needs combined with the plain view doctrine result in the particularity requirement becoming merely “correctness of paper forms,” rather than a guardian of a substantive right. Groh v. Ramirez, 540 U.S. 551, 565 n.9 (2004).

In the present case, Judge Leon issued a warrant that was limited to information “reasonably related to the investigation into the five named players’ illegal steroid use.” (R. at 3.) He was persuaded by the government to make the warrant broad enough to cover all computer

equipment and storage devices. (Id.) Circuit courts have noted this same necessity for broad search warrants for electronic sources. In United States v. Adjani, the Ninth Circuit stated, “Computer files are easy to disguise or rename, and were we to limit the warrant to such a specific search protocol, much evidence could escape discovery....The government should not be required to trust the suspect’s self-labeling when executing a warrant.” 452 F.3d 1140, 1150 (2006). Furthermore, this Court has recognized the general need for law enforcement to cast a sufficiently wide net when carrying out warrants: “a lawful search of fixed premises generally extends to the entire area in which the object of the search may be found.” United States v. Ross, 456 U.S. 798, 821 (1982). If the wide net principle means Judge Leon’s warrant was not too broad, as the District Court for the District of Wythe found, (R. at 4.), and the plain view doctrine justifies any evidence discovered in the course of the broad search, then the particularity requirement dictated by Judge Leon becomes meaningless.

It is necessary to heighten the particularity requirement in the digital evidence context and ensure that it continues to protect substantive privacy and property rights. If a warrant specifies the place to be searched and the person or things to be seized, and that “place” is a digital storage device, then magistrates should insist that law enforcement restrict themselves to the “person” and “things” described in the warrant. If it is true, as the dissenting opinion of the Fourteenth Circuit below suggests, that electronic databases, with their massive amounts of information storage and complex labeling and encryption abilities, make broad searches a law enforcement necessity, then this court must find a way to meet the need of law enforcement without jeopardizing the particularity requirement for warrants. (R. at 18.)

- B. The guidelines advocated by the Fourteenth Circuit and the Ninth Circuit in *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (2009) should be adopted by this Court.

As technology evolves, the method of applying the provisions of the Fourth Amendment should change, but the principles behind the Fourth Amendment should not. Since the plain view doctrine applied in the digital evidence context renders the particularity requirement of the Fourth Amendment meaningless, then the plain view doctrine should be altered and not the particularity requirement.

Whenever a compelling government interest conflicts with a fundamental right, this Court has stated the interest cannot “be pursued by means that broadly stifle fundamental liberties when the end can be more narrowly achieved. *Shelton v. Tucker*, 364 U.S. 479, 488 (1960). The Fourth Amendment is undoubtedly a fundamental right. *Marron v. United States*, 275 U.S. 192, 195 (1927). If the legitimate interests of law enforcement, therefore, in being able to search digital databases can be accomplished by means less compromising of Fourth Amendment liberties than the highly permissive plain view doctrine, then this court should embrace those means. Should this court affirm the Fourteenth Circuit below and find the plain view doctrine cannot apply in the digital evidence context, law enforcement does not have to be left without the necessary tools to fight crime. *United States v. Comprehensive Drug Testing* is unique and persuasive precedent, because it establishes guidelines that meet legitimate needs of law enforcement with minimal intrusion into private records.

The Ninth Circuit in *Comprehensive Drug Testing* faced a remarkably analogous set of facts to this case and developed a procedure to meet both the government’s needs and protect the players’ Fourth Amendment rights from constitutional violations. The Federal Government was investigating ten Major League Baseball players who it suspected of illegal steroid use and

obtained a warrant to search *all* “drug testing records and specimens” pertaining to Major League Baseball in the possession of Comprehensive Drug Testing, an administrator of suspicionless and statistical drug screening. Comprehensive Drug Testing, 579 F.3d at 993. The Major League Baseball Players Association moved for return of property. Because of the location of labs and specimens, the players filed motions in three different districts, and three district judges ruled in their favor. Id. All three judges went so far as to “express grave dissatisfaction with the government’s handling of the investigation.” Id. Before the Ninth Circuit, the government made a compelling case for the broad warrant and seizure, arguing the “generic hazards of retrieving data stored electronically” and relying on the plain view doctrine to justify retaining information outside the scope of the warrant. Id. at 995. The Ninth Circuit evaluated the compelling interest of law enforcement in accessing electronic data and the “grave dissatisfaction” of three district judges at the government’s gross disregard of fourth amendment protections. This was an issue of first impression for the Fourteenth Circuit below, but because of the astonishing similarity between the facts of this case and of Comprehensive Drug Testing, the Fourteenth Circuit adopted the same procedure suggested by the Ninth. (R. at 13.)

The two circuit courts organized the procedure into five practical standards for magistrates to follow when issuing a warrant for search of a digital database. The standards conform to this court’s precedent as well as with the Federal Rules of Criminal Procedure. They reflect a growing dissatisfaction among all courts with the sufficiency of traditional fourth amendment case law in the advent of technological advances. The Tenth Circuit’s holding in United States v. Carey reflected the limitations of Fourth Amendment case law in the digital context, “Relying on analogies to closed containers or file cabinets may lead courts to ‘oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive

modern computer storage.” 172 F.3d 1268, 1274 (10th Cir. 1999), *citing* Searches and Seizures of Computers and Computer Data, 8 Harv. J.L. & Tech. 75, 104 (1994). In finding a computer search exceeded the scope of a warrant, the First Circuit restricted its ruling to the facts of the case and requested that it not be dispositive of computer searches *per se*. United States v. Turner, 169 F.3d 84, 89 (1st Cir. 1999). The court expressed concern over technology’s influence on the Fourth Amendment as well.

Additionally, as Chief Justice Warren famously stated in his Lopez v. United States concurrence, “the fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual,” and “these considerations impose a heavier responsibility on this Court in its supervision of the fairness and procedures of the federal court system.” 373 U.S. 427, 441 (1963). Justice Stewart also drew attention to the changing times in Coolidge v. New Hampshire when he stated, “If times have changed, reducing every man’s scope to do as he pleases in an urban and industrial world, the changes have made the values served by the Fourth Amendment more, not less important.” 403 U.S. 443, 455 (1971). The time has come for this Court to put the issue of electronic searches to rest, and the Ninth and Fourteenth Circuits provide the best solution.

1. Magistrates should insist that the government waive reliance upon the plain view doctrine. (R. at 17.)

This issue has already been addressed in Section II, and elimination of the plain view doctrine in digital evidence searches is the first standard suggested by the lower courts. In today’s electronic age, the plain view doctrine transforms warrants for the search and seizure of electronic databases into general, “wide-ranging exploratory searches the Framers intended to prohibit.” Maryland v. Garrison, 460 U.S. 79, 85 (1987). The government should do away with

its dependence on the plain view doctrine in the digital context and adopt this standard that will once again require a search to be “carefully tailored to its justifications.” Id.

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. (R. at 17.)

This Court has frequently noted that the Fourth Amendment requires a “neutral and detached magistrate be interposed between the police and the public,” and, therefore, law enforcement is required to obtain search warrants from a magistrate prior to conducting a search. Johnson v. United States, 333 U.S. 10, 14 (1948). This is not an insult to the competency of law enforcement personnel, but it insulates fourth amendment protections from the natural impulses of law enforcement to investigate crimes. This Court has stated, “In their understandable zeal to ferret out crime and in the excitement of the capture of a suspected person, officers are less likely to possess the detachment and neutrality with which the constitutional rights of the suspect must be viewed.” Trupiano v. United States, 334 U.S. 669, 705 (1948). Furthermore, this Court stated in Marron v. United States that warrants issued by neutral magistrates should describe items to be searched and seized with such particularity that “*nothing* is left to the discretion of the officer executing the warrant.” 275 U.S. at 196. The procedure utilized when conducting searches in the digital context must actively incorporate these limitations on the discretion of law enforcement personnel.

The second standard enumerated by the Ninth and Fourteenth Circuits interposes a neutral presence between the public and law enforcement in the digital evidence context. When a law enforcement officer searches an entire personal computer, or multiple computers containing business records, to locate particular items for which she has probable cause and stumbles across

evidence of other crimes, it is understandable that she will want to investigate those crimes as well. Rather than putting officers in the position of trying to find an end around the Fourth Amendment, this standard provides them with whatever information was described in the warrant and ensures that all other information is protected.

Some might argue that this standard is unnecessary since the first standard requires police officers to forswear reliance on the plain view doctrine, so evidence found on digital sources that exceeds the evidence described in the warrant would be protected anyway. This objection does not take into account, however, the power of knowledge in investigations. Once an officer knows that the individual he or she suspected of cocaine dealing also possesses child pornography, for example, that knowledge will affect the subsequent prosecution for cocaine dealing and investigation into further criminal behavior. It is good that law enforcement officials would want to enforce the full extent of the law, but it is not good that they should be allowed to rely on knowledge that was unconstitutionally acquired when creating their investigative strategies. Again, such knowledge would incentivize officers to find a way around the Fourth Amendment instead of protecting its integrity.

3. Warrants for digital evidence must disclose the actual risks of destruction or concealment of information, as well as prior efforts to seize that information in other courts. (R. at 17.)

Information about the risks of destruction and concealment is vital to the magistrate issuing the warrant. Exigent circumstances do sometimes justify a departure from customary Fourth Amendment protocol. Ker v. California, 374 U.S. 23, 42 (1963). Magistrates should not assume exigent circumstances exist in every case, however, so if police have probable cause to suspect that information sought in the warrant will be destroyed or concealed somehow, then they should submit that in their affidavit and allow the neutral magistrate to make the determination about

how Fourth Amendment protections should apply. Police thinking there are exigent circumstances that threaten evidence does not necessarily make it so. Once again, the magistrates, not the officers, are in the best position to weigh the needs of law enforcement against the constitutional privileges of citizens.

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 non-computer personnel agents. (R. at 17.)

As this Court noted in Horton v. California, the Fourth Amendment serves a dual purposes and protects both privacy *and* property interests. 496 U.S. 128, 133 (1990). The second Comprehensive Drug Test standard protects *property* interests by ensuring that only information for which the government has probable caused can be seized. This fourth standard protects *privacy* interests to the extent that law enforcement is able to do so. If the information being sought is localized in a database, available in only certain types of files, or if technology allows for effective keyword searches, then this information should be catalogued by the government and incorporated into its search procedure. Third-party computer personnel should not review more private records than are reasonable under the circumstances, because even if they do not *seize* the "papers and effects" that come into view, they still *search* private records and this constitutes an invasion of privacy that can only be tolerated when Fourth Amendment restrictions apply. In United States v. Hill, the Ninth Circuit cautioned against blanket seizures of electronic databases and required the government to give factual proof for the necessity of a broad search in its affidavit for a warrant to search electronic media. The court said, "there must be some threshold showing before the government may 'seize the haystack to look for the needle.'" 459 F.3d 966, 975 (2006). The Comprehensive Drug Test standards provide a dual-layer of protection: the scope and method of search must be as narrowly tailored as is reasonable

under the circumstances, and third-party personnel must review all data before it is turned over to law enforcement.

5. The government must destroy, or, if the recipient may lawfully possess it, return non-responsive data, at all times keeping the court informed of its progress. (R. at 17.)

The Federal Rules for Criminal Procedure ensure this same protection in Rule 41(g), which states, “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. Crim. P. 41(g). The government is not privileged to view the non-responsive data, so if the recipient may lawfully possess it, then it should be returned or otherwise destroyed. It makes sense that law enforcement should have a means of disposing of information irrelevant to the search. “Keeping the court informed of progress” ensures compliance with these standards.

Magistrate Judge Leon’s warrant contained a particularity requirement that restricted the search to information “reasonably related to the investigation of the five named players’ illegal steroid use.” (R. at 2.) He also recognized the government need for fairly broad seizure of data and off-site search and specified that “appropriately trained personnel” should review the computer data. (*Id.*) If this court were to find today that all evidence contained in StarTests’ multiple-computer database fell within the scope of the warrant or is otherwise retainable under the plain view doctrine, then one of two results will occur: either neutral magistrates, such as Judge Leon, who value fourth amendment protections will cease issuing such broad warrants, and law enforcement will be hampered in its ability to ferret out crime, or the particularity requirement as applied to electronic data will become obsolete. When one contemplates the vast quantities of data stored on computers today, and the hundreds of millions of American citizens who have health records, financial information, personal history, and various other personal

“papers and effects” stored in private and corporate electronic databases, the urgency of the issue before the court comes into focus. Probable cause to search for evidence of crime X committed by suspect Y, for example, should not and cannot justify the search of Google’s entire record and the admissibility of evidence of other crimes committed by other suspects discovered in the course of the search. The standards adopted by the Ninth and Fourteenth Circuits protect the particularity requirement of the Fourth Amendment, and subsequently the privacy and property rights of all citizens, while still accommodating the legitimate need for law enforcement to access electronic records.

CONCLUSION

As a party aggrieved by an unlawful search and seizure, the Colonial Football League has standing along with StarTests to make a Rule 41(g) motion. Both the Respondents and the American citizens they represent have been injured by the government’s broad search of StarTests’ computer databases. Because the search is not justifiable under the plain view doctrine, the evidence seized should be returned to Respondents. Furthermore, it is necessary to heighten the particularity requirement of the Fourth Amendment in the digital evidence context to ensure that constitutionally-guaranteed rights do not fade as technology grows. The guidelines suggested by the Ninth Circuit ensure an appropriate balance between law enforcement needs and individual protections, and by adopting these standards, this Court would preserve fourth amendment privileges from further erosion in the digital evidence context.

PRAYER FOR RELIEF

For the foregoing reasons, this Court should affirm the ruling of the Fourteenth Circuit below.

Respectfully Submitted,
Counsel for the Respondent