

No. 2009-H20

In the
Supreme Court of the United States

UNITED STATES OF AMERICA,
Petitioner,

v.

STARTESTS, INC. and the COLONIAL FOOTBALL LEAGUE,
Respondents.

On Writ of Certiorari
to the Fourteenth Circuit Court of Appeals

BRIEF OF RESPONDENTS

TEAM 12

QUESTIONS PRESENTED

- I. Whether the district and circuit courts properly concluded that the CFL has standing to sue on behalf of its members when its members individually have standing to file the same claim, it is organized to protect its members' interests, and the individual members are not necessary for the lawsuit.
- II. Whether the circuit court correctly determined that plain view must be waived in digital searches because its application nullifies the Fourth Amendment warrant requirement by removing the limitations imposed by a warrant.
- III. Whether the circuit court rightly decided that the particularity requirement for warrants must be heightened in the digital evidence context because it avoids the risk of officers expanding a limited search for specific information to a general exploratory search through an individual's digital files.

TABLE OF CONTENTS

QUESTIONS PRESENTED..... ii
TABLE OF AUTHORITIES iv
OPINIONS BELOW..... 1
CONSTITUTIONAL PROVISIONS AND STATUTES INVOLVED 2
STATEMENT OF THE CASE..... 3
SUMMARY OF THE ARGUMENT 5
ARGUMENT 7
 I. THE COURTS BELOW PROPERLY CONCLUDED THAT THE CFL HAS
 STANDING BECAUSE IT SATISFIES THE TEST FOR AN ASSOCIATION TO
 HAVE STANDING TO SUE ON BEHALF OF ITS MEMBERS. 7
 II. THE CIRCUIT COURT PROPERLY CONCLUDED THAT THE FBI AGENTS
 COULD NOT SEIZE ADDITIONAL TEST RESULTS BEYOND THE SCOPE OF
 THE WARRANT BECAUSE THE PLAIN VIEW DOCTRINE SHOULD NOT APPLY
 TO DIGITAL EVIDENCE. 11
 III. THE CIRCUIT COURT PROPERLY APPLIED THE HEIGHTENED
 PARTICULARITY REQUIREMENT FOR WARRANTS IN THE DIGITAL
 EVIDENCE CONTEXT BECAUSE IT PREVENTS OFFICERS FROM
 TRANSFORMING A LIMITED SEARCH FOR SPECIFIC INFORMATION INTO A
 GENERAL WARRANT..... 17
CONCLUSION..... 25

TABLE OF AUTHORITIES

United States Constitution

U.S. Const. amend. IV	7
-----------------------------	---

United States Supreme Court Cases

<u>Arizona v. Hicks</u> , 480 U.S. 321 (1987).....	11
<u>Coolidge v. New Hampshire</u> , 403 U.S. 443 (1971)	11, 17
<u>Horton v. California</u> , 496 U.S. 128 (1990)	11
<u>Hunt v. Wash. Apple Adver. Comm’n</u> , 432 U.S. 333 (1977).....	7, 10
<u>Int’l Union, United Auto., Aerospace and Agric. Implement Workers v. Brock</u> , 477 U.S. 274 (1986).....	7, 8
<u>Maryland v. Garrison</u> , 480 U.S. 79 (1987)	20, 21
<u>Minnesota v. Dickerson</u> , 508 U.S. 366 (1993)	12, 18
<u>Pennell v. City of San Jose</u> , 485 U.S. 1 (1988).....	7
<u>Rakas v. Illinois</u> , 439 U.S. 128 (1978).....	7
<u>Smith v. Maryland</u> , 442 U.S. 735 (1979).....	9
<u>Trupiano v. United States</u> , 334 U.S. 699 (1948).....	23, 24, 25
<u>Warth v. Seldin</u> , 422 U.S. 490 (1975).....	8

Federal Cases

<u>United States v. Adjani</u> , 452 F.3d 1140 (9th Cir. 2006)	12, 22
<u>United States v. Alexander</u> , 574 F.2d 484 (8th Cir. 2009)	12
<u>United States v. Bridges</u> , 344 F.3d 1010 (9th Cir. 2003).....	22
<u>United States v. Burgess</u> , 576 F.3d 1078 (10th Cir. 2009)	15
<u>United States v. Carey</u> , 172 F.3d 1268 (10th Cir. 1999)	passim
<u>United States v. Comprehensive Drug Testing, Inc.</u> , 579 F.3d 989 (9th Cir. 2009).....	passim
<u>United States v. Dichiarinte</u> , 445 F.2d 126 (7th Cir. 1971)	12
<u>United States v. Giberson</u> , 527 F.3d 882 (9th Cir. 2008)	14, 15, 16
<u>United States v. Grimmett</u> , 439 F.3d 1263 (10th Cir. 2006)	22
<u>United States v. Hill</u> , 459 F.3d 966 (9th Cir. 2006).....	22
<u>United States v. James</u> , 353 F.3d 606 (8th Cir. 2003)	10
<u>United States v. Raney</u> , 342 F.3d 551 (7th Cir. 2003).....	12
<u>United States v. Stefonek</u> , 179 F.3d 1030 (7th Cir. 1999).....	18
<u>United States v. Stierhoff</u> , 477 F.Supp.2d 423 (D.R.I. 2007).....	15
<u>United States v. Stierhoff</u> , 549 F.3d 19 (1st Cir. 2008)	15
<u>United States v. Taketa</u> , 923 F.2d 665 (9th Cir. 1991)	9
<u>United States v. Tamura</u> , 694 F.2d 591 (9th Cir. 1982).....	18
<u>United States v. Turner</u> , 169 F.3d 84 (1st Cir. 1999).....	12, 15
<u>United States v. Walser</u> , 275 F.3d 981 (10th Cir. 2001).....	19

Federal Rules

Fed. R. Crim. P. 41(e)(2)(B).....	18
Fed. R. Crim. P. 41(g).....	7

OPINIONS BELOW

The Opinion of the United States District Court for the District of Wythe, StarTests, Inc. and the Colonial Football League v. United States, No. 2010-W20, is reprinted in the Record at R. 1. StarTests, Inc. and the Colonial Football League motioned for the return of illegally seized property under Rule 41(g) of the Federal Rules of Criminal Procedure. The government challenged the Colonial Football League's standing to sue, and argued that the evidence seized was protected under the plain view exception. The district court held that the Colonial Football League has standing to sue as an organization suing on its members behalf. It further held that the plain view exception applies to the warrant requirement, and that the warrant properly authorized the search and seizure of all StarTests, Inc. computers. It denied the 41(g) request.

The Opinion of the United States Circuit Court for the Fourteenth Circuit, StarTests, Inc. and the Colonial Football League v. United States, No. 2010-W23, is reprinted in the Record at R. 7. The circuit court affirmed the Colonial Football League's standing to sue. It rejected the plain view exception for computer searches, and held that the warrant authorizing the search of the computers was overbroad, thereby rendering the search invalid. The court reversed and remanded the district court's rejection of the Rule 41(g) motion, instructing it to issue an order for the return of all digital equipment.

CONSTITUTIONAL PROVISIONS AND STATUTES INVOLVED

The Fourth Amendment of the United States Constitution 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.

Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure provides in pertinent part:

A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant.

Rule 41(g) of the Federal Rules of Criminal Procedure provides in pertinent part:

A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return.

STATEMENT OF THE CASE

The Colonial Football League (CFL) is a member organization that contractually represents the interests of individual players and franchises within the league. R. at 10. In light of the widespread steroid controversy in other professional sports, the CFL mandated drug screening tests for all of its players in 2005. Id. at 8. Its purpose was to determine whether five percent or more of its players were using steroids so that it could enact appropriate policies for addressing the issue in the future. Id. at 1.

To conduct these tests, the CFL hired StarTests, Inc., an independent business specializing in conducting drug tests for professional sports franchises, school districts, corporations, and other organizations. Id. The CFL paid for both the tests and the storage of the information. Id. at 10. Prior to conducting the tests, both the CFL and StarTests informed the players that their private information would remain confidential and anonymous. Id. at The only information intended for release was the numerical percentage of players testing positive for steroid use. Id. at 8.

In July 2008, the Federal Bureau of Investigation (FBI) began an investigation into the steroid usage by the players in numerous major professional sports leagues. Id. at 1. During its investigation, the FBI discovered evidence implicating five players in the CFL as distributors and users of steroids. Id. It also learned of the CFL's drug testing program. Id. at 8.

In furtherance of its investigation, the FBI sought a search warrant from the magistrate to procure information related to these five players. Id. It requested a broad warrant allowing for the search and seizure of all of StarTests' computer records, files, and equipment relating to the CFL. Id. As a justification for the large scope of its request, the FBI emphasized several unique aspects of computers, including their ability to hold massive quantities of data, the difficulty of

locating and obtaining the files, and the fact that different software may be needed to view the files. Id. at 2.

The magistrate issued a warrant authorizing the “search [of] computer equipment, storage devices, and – where an on-site search would be impracticable – [seizure of] either a copy of all data or the computer equipment itself.” Id. at 8. The warrant restricted the FBI to information “reasonably related to the investigation into the five named players’ illegal steroid use.” Id. It required that “law enforcement personnel trained in searching and seizing computer data” determine when it was necessary to seize and remove the computer equipment. Id. “Appropriately trained personnel” were charged with reviewing the data, retaining the information relevant to the search, and marking the irrelevant data and equipment for return. Id.

On November 1, 2008, the FBI executed the search warrant on a StarTests facility. Id. at 2. StarTests personnel indicated that in order to protect confidentiality, there were three unique CFL databases saved on three separate computers. Id. The three databases had to be cross-referenced with one another to interpret the test result data. Id. & n.1. The computer forensics agent made the decision to seize all of the computer equipment at the facility by copying the hard drives. Id. at 2.

Over the next few weeks, the FBI searched the copied data. In the course of the search, it found the five players’ test results. Id. at 9. It also discovered positive test results for both illegal steroid usage and other narcotics and marijuana use by many other players in the league. Id. The agent conducting the search copied and retained this information. Id. The FBI subsequently announced that it was expanding the scope of its investigation to include illegal substance abuse. It later returned the unnecessary hard drives and computer equipment. Id.

SUMMARY OF THE ARGUMENT

The decision of the circuit court should be affirmed in all respects. The circuit court properly affirmed the district court's holding that the CFL has standing to sue on behalf of its members through the organizational standing test articulated by this Court in Hunt v. Wash. Apple Adver. Comm'n. First, its members would individually have standing to file the same claim because they each have the right to seek the return of their own drug test data as aggrieved parties under Rule 41(g) of the Federal Rules of Criminal Procedure. Second, the CFL is a member organization charged with protecting its members' individual interests. Finally, the individual members are not necessary for the lawsuit because the remedy sought is the return of drug test data owned by the CFL.

The circuit court also correctly held that officers must forego the use of the plain view doctrine in digital searches and seizures. The plain view doctrine serves as a way to nullify the Fourth Amendment warrant requirement in digital evidence cases. Its application enables officers to broaden the scope of a warrant beyond its limitations, thereby transforming a limited and specific search into a general rummaging through a person's electronic files.

Even if this Court finds that plain view should apply to digital searches, its application in this case goes beyond the scope of material ordinarily addressed by the doctrine. Government officials cannot use plain view as a justification for expanding the scope of an authorized search. In this case, as soon as the FBI discovered evidence of drug use beyond the steroid data for the five players addressed in the warrant, it illegally expanded the scope of its search to cover all drug use without procuring a second warrant authorizing the expansion. The Fourteenth Circuit's recognition of this expansion as a danger led to its adoption of the rule precluding the use of plain view in such instances, and its rule should be upheld.

Finally, the circuit court rightly decided to apply a heightened particularity requirement in the digital evidence context because it avoids turning a limited search for information into a general exploratory search for evidence. Because there is a heightened potential for intermingling documents in computer evidence, the circuit court properly adopted the Ninth Circuit's guidelines for issuing and executing search warrants for digital evidence cases. Although the FBI returned unneeded data, it failed to satisfy the guidelines in several other ways. First, the officer collaborated with a computer forensics agent in conducting an extensive review of the CFL's database. Second, the FBI omitted information regarding the risk of destruction and concealment of data when it sought the warrant from the magistrate. Finally, as indicated above, it unlawfully expanded the scope of the warrant when it turned its attention to drug use by players other than the five at issue in the investigation.

Despite the FBI's contention that federal magistrates may issue warrants authorizing the seizure of all computer equipment and files for later sorting, it fails to acknowledge the fundamental importance of striking a balance between law enforcement's need for information and private individuals' privacy interests. This Court should affirm the Fourteenth Circuit's decision authorizing a heightened particularity standard so as to enable the Fourth Amendment's longstanding protection against unreasonable governmental intrusion to adequately protect these interests in the digital age.

ARGUMENT

I. THE COURTS BELOW PROPERLY CONCLUDED THAT THE CFL HAS STANDING BECAUSE IT SATISFIES THE TEST FOR AN ASSOCIATION TO HAVE STANDING TO SUE ON BEHALF OF ITS MEMBERS.

The CFL has standing to sue because its members individually have standing to file the same claim, it is organized to protect its members' interests, and the individual members are not necessary for the lawsuit. A party who motions for the return of illegally seized property through Rule 41(g) must be the party who was "aggrieved by an unlawful search and seizure of property or by the deprivation of the property." Fed. R. Crim. P. 41(g). The Fourth Amendment protects the rights of the people against unreasonable searches and seizures. U.S. Const. amend. IV. It also guards against unreasonable intrusion by the government into places in which people have a "legally significant interest," including places outside of one's home. Rakas v. Illinois, 439 U.S. 128, 142 (1978).

As a general rule, Fourth Amendment rights are personal rights. Id. at 133-34 (citations omitted). Though these rights ordinarily cannot be vicariously asserted, id., associations may have standing to sue on their members' behalf. Pennell v. City of San Jose, 485 U.S. 1, 7 (1988). A three-prong test is used to determine whether an association has standing to sue on behalf of its members. Int'l Union, United Auto., Aerospace and Agric. Implement Workers v. Brock, 477 U.S. 274, 282 (1986). Standing exists when "(a) its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to the organization's purpose; and (c) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit." Id. (quoting Hunt v. Wash. Apple Adver. Comm'n, 432 U.S. 333, 343 (1977)) With respect to the relief sought, injunctions, declarations, or other forms

of prospective relief are usually of such a nature that the members' involvement in the suit is not necessary. Warth v. Seldin, 422 U.S. 490, 515 (1975).

Organizations that satisfy this test are deemed to have standing to sue on behalf of their members. For instance, this Court held in Brock that a trade union had standing to challenge a statute that allegedly resulted in a denial of certain unemployment benefits to many of its members. Brock, 477 U.S. at 290. It explained that at least some of the members had individual standing to sue because they were injured by the denial of their allowances under the law. Id. at 285-86. The Court further found that the interests of those individuals were germane to the organization's purpose due to the fact that a trade union exists to protect the employment-related interests of its members. Id. at 286-87. Finally, the Court determined that the individual members had no need to take part in the lawsuit because the union was capable of representing all of their interests. Id. at 287-88.

The relief sought is an important consideration for determining whether the participation of the individual members of an organization is needed for a lawsuit. In Warth v. Seldin, the Court held that a home builders association attempting to join as a plaintiff in a suit did not have standing because the relief sought was monetary damages. Warth, 422 U.S. at 515. The Court reasoned that the damages, if awarded, would have to go to specific individuals who were directly harmed, meaning that each aggrieved member was a necessary part of the suit. Id. at 515-16. It noted that in seeking damages, the association alleged neither pecuniary injury to itself nor assignment of any of its members' damages claims. Id. at 515.

The CFL satisfies this test because the players involved have a basis for their own standing to sue, protecting their rights is part of the CFL's job, and the individual players are not needed in the action. The first prong is satisfied because the FBI seized numerous players' drug

test records, and they, as parties aggrieved by the search, would have the right to seek the return of these records under Rule 41(g) upon a showing that they were illegally seized. The second prong is also met because of the nature of the CFL. As the district court pointed out, the organizational purpose of the CFL is to protect the interests of its players, including their privacy interests. Like the trade union in Brock, the CFL's obligation to protect these interests relates directly to its purpose. Lastly, the relief demanded in this case is the return of the drug test records on the StarTests computers. Unlike the monetary damages sought in Warth, this is a request for prospective relief along the lines of the relief sought in Brock. The members of the CFL need not be individually involved in a suit where the remedy, if granted, is the return of drug test data and samples to the organization charged with protecting their privacy.

The government argues that the CFL lacks standing because it is a party seeking to challenge the search of another party's office, rather than a party aggrieved by the search.¹ To make a valid Fourth Amendment claim, an aggrieved party must have "a subjective expectation of privacy that is objectively reasonable." United States v. Taketa, 923 F.2d 665, 671 (9th Cir. 1991) (citing Smith v. Maryland, 442 U.S. 735, 740 (1979)). This means that the individual must be seeking to preserve something he or she expected to be private, and that the expectation of privacy is justifiable under the circumstances. Smith, 442 U.S. at 740. The government ultimately contends that the CFL lacked a reasonable expectation of privacy in the StarTests computers.

¹ The holdings of both the district and circuit courts referenced language in Rakas v. Illinois articulating the 'target theory,' effectively making the victim of a search the person against whom the search was directed. Rakas, 439 U.S. at 134-35 (1978) (quoting Jones v. United States, 362 U.S. 257, 261 (1960)). Both opinions below incorrectly cite the theory as the holding of Rakas, but this language was labeled as dicta and expressly rejected shortly after it was quoted. See Rakas, 439 U.S. at 135. This does not, however, change the analysis here because the three-prong test is still controlling. See Brock, 477 U.S. at 282.

The problem with this argument is twofold. First, as illustrated by the application of the associational standing test, the CFL's *members*, not necessarily the CFL itself, must individually have the right to seek the relief at issue. *See, e.g., Hunt*, 432 U.S. at 344 (holding that a commission suing on behalf of a number of aggrieved apple growers had standing to sue when the injuries averred were only suffered by the members individually). In this case, as the district and circuit courts observed, the individual players affected would each have standing to file a 41(g) motion for the return of the seized information under the language of the rule itself because they were the aggrieved parties. The CFL told them that any information collected would remain confidential and anonymous, which gave them an expectation of privacy. The information's sole function was to help determine whether the CFL needed to conduct regular drug testing, so a reasonable player in their position would expect that the data would only be used for that purpose. Whether the CFL was the aggrieved party with a reasonable expectation of privacy is immaterial, therefore, because the players themselves had such an expectation.

Second, even if the players did not have this expectation, the CFL nonetheless has a privacy interest in the records that are stored at StarTests because the information seized belongs to the CFL, not to StarTests. The circuit court emphasized that the CFL's ownership interest in the databases is arguably stronger than StarTests'. R. at 10. Though StarTests actually performed the drug tests and stored the records, it did so at the request of the CFL, which paid for these services. The records produced by StarTests are thus property of the CFL, and StarTests' only remaining connection to these records is that it is merely storing them for the CFL. *See United States v. James*, 353 F.3d 606, 614 (8th Cir. 2003) (“[O]ne does not cede dominion over an item to another just by putting him in possession.”)

The CFL satisfies both the associational standing test and Rule 41(g) as an aggrieved party due to its ownership interest in the test results. As such, the district and circuit courts correctly concluded that it has standing to seek the return of the data as plaintiffs in this case, and their holdings should be affirmed.

II. THE CIRCUIT COURT PROPERLY CONCLUDED THAT THE FBI AGENTS COULD NOT SEIZE ADDITIONAL TEST RESULTS BEYOND THE SCOPE OF THE WARRANT BECAUSE THE PLAIN VIEW DOCTRINE SHOULD NOT APPLY TO DIGITAL EVIDENCE.

The plain view doctrine cannot properly be used to seize digital evidence because its application nullifies the constitutional warrant requirement and serves as a justification for exploratory or general searches of digital storage devices. Plain view functions primarily as a means by which police may conduct a warrantless seizure of evidence in the course of a proper search. Horton v. California, 496 U.S. 128, 133-34 (1990). It is not an exception to the warrant requirement for searches. Id. at 133. Instead, it allows officers to legally seize evidence that they can clearly see once a search is justified by a warrant or some exception to it. *See* Coolidge v. New Hampshire, 403 U.S. 443, 467-68 (1971) (plurality opinion). Officers cannot use the plain view doctrine to “extend a general exploratory search from one object to another until something incriminating at last emerges.” Id. at 466.

The requirements for a seizure to satisfy the plain view doctrine are well settled. To show that seized evidence was in plain view, a three-step analysis is conducted: (1) the officer must observe the evidence from a lawful vantage point, (2) the officer must have a “lawful right of access to the object itself,” and (3) the incriminating character of the evidence must be immediately apparent. Horton, 496 U.S. at 136-37.

The third element is functionally the probable cause requirement in plain view cases. Arizona v. Hicks, 480 U.S. 321, 327 (1987). Police generally lack probable cause to believe that something in plain view is contraband if a further search of the object must be conducted to determine whether its character is actually incriminating. Minnesota v. Dickerson, 508 U.S. 366, 375 (1993) (citations omitted). In some cases, documents that must be opened and read before their criminal character becomes apparent are not considered to be in plain view. See United States v. Dichiarinte, 445 F.2d 126, 131 (7th Cir. 1971) (holding that personal documents seized during search with consent for narcotics were not in plain view and could not be used in later tax evasion proceedings).

The various circuits' interpretations of the plain view doctrine's applicability to digital searches are inconsistent. Some courts are very willing to apply plain view in this context, while others are opposed or hesitant to do so. Compare United States v. Raney, 342 F.3d 551, 558 (7th Cir. 2003) (concluding that a search of a computer for child pornography was within the scope of consent to search a home for evidence related to child erotica) with United States v. Alexander, 574 F.2d 484, 490-91 (8th Cir. 2009) (noting that a discovery of child pornography during a validly authorized search of a computer was protected by the plain view doctrine) and United States v. Turner, 169 F.3d 84, 88 (1st Cir. 1999) (finding that a search of a computer during an investigation of an apartment with the owner's consent to search for physical evidence of an assault exceeded the scope of consent); see also United States v. Carey, 172 F.3d 1268, 1276 (10th Cir. 1999) (applying plain view indirectly to one image of child pornography accidentally discovered while searching a computer for drug trafficking information). Some courts suggest that analogizing computers to brief cases or other closed containers overlooks the necessary reality that computers *are* different. See United States v. Adjani, 452 F.3d 1140, 1152 (9th Cir.

2006) (“Computers are simultaneously file cabinets (with millions of files) and locked desk drawers; they can be repositories of innocent and deeply personal information, but also evidence of crimes.”). Significantly, the Ninth Circuit recently established five standards for magistrates issuing warrants in digital searches. United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1004-06 (9th Cir. 2009). The first of these specifically requires that the government waive plain view in such cases. Id. at 1006.

The Fourteenth Circuit Court of Appeals relied on and adopted the Ninth Circuit’s statement that plain view cannot be used in computer cases. In Comprehensive Drug Testing, the FBI seized computer drug test data after learning through its ongoing investigation that several Major League Baseball players tested positive for steroids. Id. at 993. The court held that plain view cannot be used in computer searches because of the breadth it would create. Id. at 998. It explained that if plain view applies to computer searches, every warrant to search for electronic information effectively becomes a general warrant. Id. at 1004. Electronic files must be opened to determine whether they are covered by the scope of a warrant, necessarily placing them in the plain view of the officer reviewing the file. Id. at 1004-05. This creates a justification for officers to seize and claim as evidence anything found while searching for a single file, thereby nullifying any need for a warrant. Id. at 998.

Some circuits apply plain view without addressing what constitutes plain view in digital information cases. For example, in United States v. Carey, the Tenth Circuit held that a detective searching a computer for child pornography exceeded the scope of a warrant authorizing him to search for drug related evidence. Carey, 172 F.3d at 1276. The warrant’s scope extended only to computer files related to drug trafficking. Id. at 1272-73. The court indicated that, based on the officer’s own testimony, upon inadvertently discovering the first image of child pornography, the

officer temporarily abandoned his search for drug material and started searching for more pornography. Id. at 1273. It found that the officer acted outside the authorized scope of the warrant when he actually turned his attention to a search for child pornography. Id. As a result, the court suppressed any child pornography images found during the subsequent search, though it did not suppress the first image. Id. at 1273 & n.4. A concurring opinion explained that the child pornography search was improper because the officer specifically turned his attention toward finding it without getting a new warrant. Id. at 1276-77 (Baldock, J., concurring).

Applying plain view to digital searches justifies an improper expansion of the scope of the search and nullifies the need for a warrant. Like the Comprehensive Drug Testing situation, the officers here used the protection of a broad warrant to seize files stored on StarTests' hard drives. The important limitation in this warrant is that the search covered only information reasonably connected to the investigation of the five named players' steroid usage. Like the search in Carey, when the FBI discovered the additional drug use information, the scope of the search was expanded without the procurement of a new warrant. Searching the files brought every document saved on the seized or copied hard drives into plain view. In effect, just as the Comprehensive Drug Testing court feared, applying the plain view doctrine renders the warrant's limitations meaningless.

The government contends that computers should not receive heightened Fourth Amendment protection, and that plain view should apply to digital evidence searches because the files were searched pursuant to a valid warrant. Some courts resist affording heightened protection to computer searches. *See, e.g., United States v. Giberson*, 527 F.3d 882, 888-89 (9th Cir. 2008) (“[T]he potential intermingling of materials [in a computer] does not justify an exception or heightened procedural protections for computers beyond the Fourth Amendment’s

reasonableness requirement.”). A prevailing view in some circuits is that a search of a computer is valid as long as the authorizing warrant is valid. See United States v. Burgess, 576 F.3d 1078, 1090 (10th Cir. 2009). Circuits applying plain view to electronic searches typically focus heavily on the scope of the warrant or the consent to search. See Turner, 169 F.3d at 88; see also United States v. Stierhoff, 477 F.Supp.2d 423, 444-49 (D.R.I. 2007), *aff’d* 549 F.3d 19 (1st Cir. 2008). Even under this approach, however, plain view only covers evidence discovered while an officer is searching for items or files within the area authorized. See, e.g., Giberson, 527 F.3d at 887-88;.

When applied to computer searches, plain view tends to authorize warrantless searches of folders where the information sought is likely stored. For instance, in United States v. Stierhoff, the District Court for the District of Rhode Island held that evidence of tax evasion located in a folder on a computer was beyond the scope of consent given to search, and thus unprotected by the plain view doctrine. Stierhoff, 477 F.Supp.2d at 449. The defendant’s consent authorized officers to search a specific folder, and the officers gave no indication that the search would extend to other folders. Id. at 443. The court analogized the folder that was opened without consent to a closed container. Id. at 445. It reasoned that the label given to the folder had many possible meanings, thereby distinguishing it from cases where things like firearm containers were clearly labeled to suggest the presence of a gun inside. Id. at 445-46. Because the label of the folder in front of the officers was not clearly facially incriminating, it failed the incriminating nature prong of the plain view test. Id. at 448-49.

Prior to its ruling in Comprehensive Drug Testing, the Ninth Circuit addressed a somewhat similar situation to Stierhoff, leading to a different result. In United States v. Giberson, a computer specialist searching a “mirror image” of the defendant’s hard drive for image files related to the production of false identification cards discovered child pornography

among the saved files on the hard drive. Giberson, 527 F.3d at 885. The program used in the search allowed the specialist to view small versions (thumbnails) of many of the images on the computer simultaneously. Id. The specialist printed out the pornographic images as he came across them without procuring a second warrant in continuing his search for the identification card files. Id. The court held that the pornography was within the scope of the authorized search for image files on the computer. Id. at 899. Without directly applying the plain view doctrine, the court explained that it was unreasonable to require officers to trust a defendant's labeling of files and folders on a computer because of the ease with which they can be mislabeled or hidden. Id. at 889-90. The child pornography was seizable, it reasoned, because the files were discovered without the officer deviating from the scope of the authorized search. Id. at 890.

Applying the plain view doctrine as articulated in Stierhoff to this case, it initially seems that the government's search for information pertaining to marijuana and other narcotics was proper. The files through which the officer searched were all related to the storage of drug test data, which, unlike the separated folder in Stierhoff, contained both relevant and irrelevant information. Like the files in both Stierhoff and Giberson, the files searched in this case were within the scope of the warrant. Because the files were initially located during the authorized search, they are more analogous to those in Giberson and less like those in Stierhoff. However, the FBI's expansion of the search upon finding the evidence of non-steroid drug use makes this case distinguishable from Giberson and aligns it with Carey. The FBI, unlike the officers in Giberson, began specifically looking for data related to all illegal drug possession and sale within the CFL. This was not within the authorized scope of the warrant. Any non-steroid drug data accessed by the officers became the target of the search instead of a discovery made during an authorized search.

Additionally, even assuming that this Court applies plain view to digital searches, the information seized here was not in plain view. Though the lawful vantage point and lawful right of access prongs of the test are probably satisfied by the warrant, the search fails the third prong because the incriminating nature of the files was not immediately apparent. The files were stored on three separate hard drives, and the players were only identified by a number in the file with the test results. Furthermore, many of the files were either encrypted or hidden on other external drives. Unlike the first child pornography image located in Carey and the various images located in Giberson, the files here needed to be opened and viewed, and even then, some of them had to be decrypted in order to discern their contents. This illustrates that the files, like the folder in Stierhoff, were not facially incriminating. In fact, they are less incriminating than the Stierhoff folder because discerning their nature required cross-referencing them with information stored on completely separate computers as opposed to simply opening them.

Application of the plain view doctrine transforms targeted, authorized searches into general searches and nullifies the need for a warrant in the process. The Fourteenth Circuit properly recognized this reality in its adoption of the Ninth Circuit's Comprehensive Drug Testing standard, and its decision should be upheld.

III. THE CIRCUIT COURT PROPERLY APPLIED THE HEIGHTENED PARTICULARITY REQUIREMENT FOR WARRANTS IN THE DIGITAL EVIDENCE CONTEXT BECAUSE IT PREVENTS OFFICERS FROM TRANSFORMING A LIMITED SEARCH FOR SPECIFIC INFORMATION INTO A GENERAL WARRANT.

The particularity requirement for warrants must be heightened in the digital evidence context because it prevents officers from transforming a limited search for particular information into a general exploratory search for evidence. In Coolidge v. New Hampshire, the United States Supreme Court explained the Fourth Amendment's warrant requirement. Coolidge, 403 U.S. at

467. First, it provides a check to ensure that there is probable cause to conduct a search by requiring the approval of a magistrate. Id. Second, it prevents officers conducting the search from performing a “general, exploratory rummaging in a person’s belongings . . . by requiring a ‘particular description’ of the thing to be seized.” Id. Where an officer executes a valid warrant for one item and seizes a different item, the Court is aware of the danger of officers enlarging “a specific authorization, furnished by a warrant . . . into the equivalent of a general warrant to rummage and seize at will.” Dickerson, 508 U.S. at 378 (citing Brown, 460 U.S. at 748). The significance of the particularity requirement is that it ensures that officers executing a search warrant stay within the bounds established by the magistrate. United States v. Stefonek, 179 F.3d 1030, 1033 (7th Cir. 1999).

The danger of turning a specific authorization to search or seize into a general warrant has been addressed in the pre-digital context. The Ninth Circuit recognized that, while all items in a file may be searched subject to specific guidelines, seizing items not described in a warrant for later inspection is more intrusive. *See, e.g., United States v. Tamura*, 694 F.2d 591, 595-96 (9th Cir. 1982) (holding that a wholesale seizure of all of a company’s accounting records, while valid, was a close case for the abuse of the warrant’s authority by potentially transforming it into a general warrant). This is especially important in cases where documents “are so intermingled that they cannot feasibly be sorted on site.” Id. In such cases, documents should be sealed and held until a magistrate approves a further search. Id. The Federal Rules of Criminal Procedure were recently amended to authorize an off site review of seized digital evidence. Fed. R. Crim. P. 41(e)(2)(B).

While Tamura provides Fourth Amendment protections from general warrant searches and seizures in the pre-digital context, the protections are not feasible and must be heightened for

digital evidence because of the inherent nature of computer media. The Tenth Circuit recognized the difficulties surrounding computer evidence in United States v. Walser, 275 F.3d 981 (10th Cir. 2001). The capability of computers to hold massive quantities of information about an individual's personal life and business creates a heightened potential for the intermingling of documents. Walser, 275 F.3d at 986. In recognition of this, some courts require officers to separate the files and search only those that fall within the scope of the warrant. *See* Carey, 172 F.3d at 1275.

Because of this heightened potential for the intermingling of documents in computer evidence, the Ninth Circuit formulated requirements directing the issuance and execution of search warrants for computer data. In addition to insisting that the government waive reliance on the plain view doctrine, magistrates issuing search warrants to examine computer data that could ultimately result in the seizure of computer equipment must observe all of the following guidelines:

(2) segregation and redaction must either be done by specialized personnel or an independent third party, (3) warrants and subpoenas must disclose the actual risk of destruction of information as well as prior efforts to seize that information in other judicial fora, (4) 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) 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, 579 F.3d at 1006.

The Fourteenth Circuit relied on and adopted the Ninth Circuit's guidelines for issuing and executing search warrants in digital evidence cases. In Comprehensive Drug Testing, the FBI seized and reviewed computer drug testing data for hundreds of Major League Baseball

players pursuant to a warrant only allowing it to seize and review “all drug testing records and specimens” for ten players for whom the government had probable cause. Id. at 993. The court held that the FBI disregarded the players’ constitutional rights by failing to comply with the warrant’s requirement to have designated computer personnel screen and segregate information, and by failing to return computer data collected for other baseball players for whom the government lacked probable cause. Id. at 996-97. The court also held that the government failed to fairly disclose the risk of concealment and destruction of evidence. Id. at 998. It reasoned that the government’s failure to mention that Comprehensive Drug Testing agreed to keep the data intact until there was a ruling on a subpoena created the false impression that the computer data had to be seized or else it would be lost. Id. The court explained that a lack of candor by the government “bears heavily against” it in deciding a motion to return seized data. Id. at 999. Additionally, the court held that in segregating the seizable from non-seizable data, the government neglected to adhere to and achieve the purpose of the warrant to obtain evidence relating to the ten players for whom it had probable cause by seizing the entire directory containing data on hundreds of baseball players. Id.

Decisions by other courts offer support for the Ninth Circuit’s general fear of turning a limited search for evidence into a general warrant. For example, in United States v. Carey, the Tenth Circuit held that a detective’s search of a computer resulting in the search and seizure of evidence pertaining to child pornography exceeded the scope of the warrant. Carey, 172 F.3d at 1276. The court reasoned that based on the evidence, the detective was aware that each time he opened a file containing child pornography, he was expanding the scope of the warrant beyond its limitation to computer evidence concerning drug activity. Id. at 1272-73. Additionally, in Maryland v. Garrison, 480 U.S. 79 (1987), the United States Supreme Court held that a search

warrant was validly issued even though hindsight proved that the warrant's description was broad. Id. at 85-86. The Court reasoned that a search of one of two apartments pursuant to a broad issuance and execution of the warrant describing only one apartment on the third floor was the result of an honest mistake even after the officers made adequate inquiries into the construction of the apartment complex. Id. at 86.

This case illustrates the very disregard for constitutional rights that both the Ninth and Fourteenth Circuits resisted regarding the transformation of a limited search warrant for digital evidence into a general warrant. Analogous to the situation in Comprehensive Drug Testing, the officers here failed to satisfy several of the heightened particularity requirements for issuing and executing warrants for computer evidence. The warrant issued here imposed restrictions on the FBI to have trained law enforcement personnel decide when computer equipment should be seized and removed from the premises. Other trained personnel were to review the data in order to decide which information to keep and which to return. Ultimately, like the officers in Comprehensive Drug Testing, the personnel deciding when to seize the computer equipment collaborated with the FBI in conducting an extensive search of the CFL's database.

Additionally, while the evidence is unclear as to whether the FBI was required to provide information concerning the risks of destruction or concealment of data, the risk of destruction is not apparent. The concealment of information in the database is no different from the electronic files in Comprehensive Drug Testing. It is consistent with the very objective of the testing required by the CFL and conducted by StarTests, which was to maintain confidentiality while simultaneously determining the prevalence of steroid usage in the league.

Finally, though the FBI returned the unneeded computer equipment and data as required by the warrant, it failed to adhere to the general scope of the warrant limiting the search to the

five players for whom the FBI had probable cause. The FBI did not make an honest mistake like the officers in Garrison. Instead, it had the opportunity to search the CFL databases for weeks. The FBI returned the unneeded equipment and data only after copying and retaining both the information concerning the five players involved and the information pertaining to the marijuana and narcotics use by other players in the league. Once this information was in its possession, the FBI made its announcement expanding the scope of the investigation. The FBI displayed the same degree of awareness prior to expanding the scope of the warrant beyond the five players as the officers in both Comprehensive Drug Testing and Carey. The expansion of the scope of the search in this case is thus indistinguishable from the improper expansions in those cases.

The government contends that federal magistrates should issue warrants authorizing the seizure of all computer equipment and files for later sorting, thereby rejecting a heightened particularity requirement in the digital evidence context. When met with a particularity challenge the courts have taken a relatively forgiving stance. *See* United States v. Grimmett, 439 F.3d 1263, 1269 (10th Cir. 2006). The particularity standard outside of the digital context is reasonable particularity, which varies depending on the items to be seized and the other circumstances of the case. *See* United States v. Bridges, 344 F.3d 1010, 1016 (9th Cir. 2003).

With respect to digital evidence, there is a general mistrust of relying on a suspect's labeling of files in executing a warrant because computer files can easily be disguised and renamed, thereby limiting law enforcement's ability to procure evidence in criminal cases. *See, e.g.,* Adjani, 452 F.3d at 1150 (explaining that limiting a search warrant to specific search protocol risks overseeing evidence because of defendant's self-labeling of computer files). Courts accepting the practicality of broad search and seizure authority generally require a showing of difficulty in obtaining computer evidence before the government may, "seize the

haystack to look for the needle.” United States v. Hill, 459 F.3d 966, 975 (9th Cir. 2006). The Comprehensive Drug Testing standard clarifies this requirement by setting out its specific guidelines for issuing and executing warrants in digital evidence cases. Comprehensive Drug Testing, 579 F.3d at 1006.

The government’s argument against the heightened particularity standard addresses the difficulties posed by obtaining a limiting warrant for digital searches. It forces reliance upon the self-labeling of files by defendants, the same danger recognized by both the Giberson and Adjani courts. If the particularity of the warrant is too narrow, officials may be unable to locate significant evidence simply because it was hidden away in a folder with an innocent name.

While gathering evidence is an important concern, the heightened particularity requirement achieves a fair balance between the needs of law enforcement and the individual’s constitutional privacy interest. It does not prevent searches and seizures of computers. To the contrary, a search of a computer may be fairly extensive. The protocol prescribed by the Ninth Circuit and adopted by the Fourteenth Circuit functions to protect the privacy interests of individuals while still allowing government officials to achieve the evidence they seek. If an individual unrelated to the case conducts a search of the files, he or she can adequately separate them and turn over only that information for which the government has probable cause. The only significant loss that this causes is that the government is compelled to forego plain view. In this situation, it is a necessary sacrifice if the Fourth Amendment is to properly function in the digital age.

Adoption of the Ninth Circuit’s heightened particularity requirement for warrants in the digital evidence context has the overall benefit of reinforcing the longstanding tradition of the Fourth Amendment to protect both the innocent and guilty from governmental intrusions while

maintaining the necessary processes of officers. *See Trupiano v. United States*, 334 U.S. 699, 709 (1948). The Fourth Amendment's fundamental requirement that a warrant particularly describe the items to be seized prevents officers from freely ascertaining for themselves the scope of a search. *Id.* at 710. Because the risk of over-seizing data is heightened in the digital context, there is greater necessity for magistrates to be vigilant in issuing warrants, so that the procedure for sorting electronic data does not become a medium for the government to evade the ordinary citizen's privacy interest. *Comprehensive Drug Testing*, 579 F.3d at 1005.

The Fourteenth Circuit's application of the heightened particularity requirement for digital evidence should therefore be affirmed because it fosters the attainable and necessary balance between law enforcement's need for information and the individual citizen's right to privacy, while simultaneously preserving the fundamental traditions of the Fourth Amendment.

CONCLUSION

This case illustrates two interconnected challenges faced by the law in light of technological advancements. First, the use of plain view poses the threat of broadening the scope of an already broad warrant. “The Fourth Amendment was designed to protect both the innocent and the guilty from unreasonable intrusions upon their right of privacy while leaving adequate room for the necessary processes of law enforcement.” Trupiano, 344 U.S. at 709-710. Applying plain view in digital search cases effectively authorizes officers conducting a search to go on a fishing expedition through electronic files. In this case, the expedition yielded a fish in the form of the additional drug usage data. Under the government’s interpretation of plain view, this information authorized an expansion of the search beyond the warrant’s limitations. As a result, plain view nullified the Fourth Amendment’s warrant requirement by rendering its limitations meaningless.

Second, with the emergence of the digital age, there is a heightened risk of intermingling documents stored electronically. This case asks the Court to strike an important balance. Electronic storage is a way of life, and though the incentive exists for wrongdoers to disguise digital files, there is nonetheless a need to guard against unreasonable governmental intrusions into individuals’ privacy. In addition to foregoing plain view, a heightened particularity requirement in the digital evidence context offers a viable balance between the government’s need for information and the ordinary citizen’s privacy interest.

For these reasons, the Respondents respectfully request that the decision of the Fourteenth Circuit be affirmed and the illegally seized evidence ordered returned under Rule 41(g).